CERT® Resilience Management Model

A Maturity Model Approach to Managing Operational Resilience

SEI Webinar Series
28 July 2010

Rich Caralli
Technical Manager – CERT Resilient Enterprise Management Team

© 2010 Carnegie Mellon University

Report Documentation Page

Form Approved
OMB No. 0704-0188

Public reporting burden for the collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to a penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number.

1. REPORT DATE
28 JUL 2010

2. REPORT TYPE

3. DATES COVERED
00-00-2010 to 00-00-2010

4. TITLE AND SUBTITLE
CERT Resilience Management Model: A Maturity Model Approach to Managing Operational Resilience

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
Carnegie Mellon University ,Software Engineering Institute,Pittsburgh,PA,15213

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)

10. SPONSOR/MONITOR’S ACRONYM(S)

11. SPONSOR/MONITOR’S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT **unclassified**	b. ABSTRACT **unclassified**	c. THIS PAGE **unclassified**	**Same as Report (SAR)**	**76**	

Introduction

Rich Caralli

Technical Manager – CERT Resilient Enterprise Management Team

25+ years in IT Audit and IT Management in financial services, manufacturing, and energy

8 years @ SEI concentrating in information security risk management

BS-Accounting; MBA

Frequent lecturer in Carnegie Mellon Heinz School and CIO Institute

© 2010 Carnegie Mellon University

Agenda

What is CERT-RMM?

History

Model Building Blocks

Model Architecture

The Capability Dimension

Determining Capability

CERT-RMM Credentialing

CERT-RMM and PS-Prep

CERT-RMM Product Suite

© 2010 Carnegie Mellon University

What is CERT®-RMM?

The CERT® Resilience Management Model (CERT-RMM) is a capability model for managing and improving operational resilience.

- Positions **operational resilience** in a process improvement view
- Includes 26 **“process areas”**
- Focuses on the operations phase of the lifecycle
- Defines “maturity” through “capability levels” consistent with CMMI
- Uses CMMI architecture for ease of adoption
- Includes a “continuous representation” for agile adoption

© 2010 Carnegie Mellon University

Distinguishing features of CERT®-RMM

CERT-RMM brings several innovative and advantageous concepts to the management of operational resilience.

- **The convergence advantage:** merging the disciplines of security, BC/DR, and IT ops into a single model
- **The process advantage:** elevating these disciplines to a process view, useful as an integration and measurement framework
- **The maturity advantage:** provides a foundation for practical institutionalization of practices—critical for retaining these practices under times of stress

© 2010 Carnegie Mellon University

History of CERT-RMM

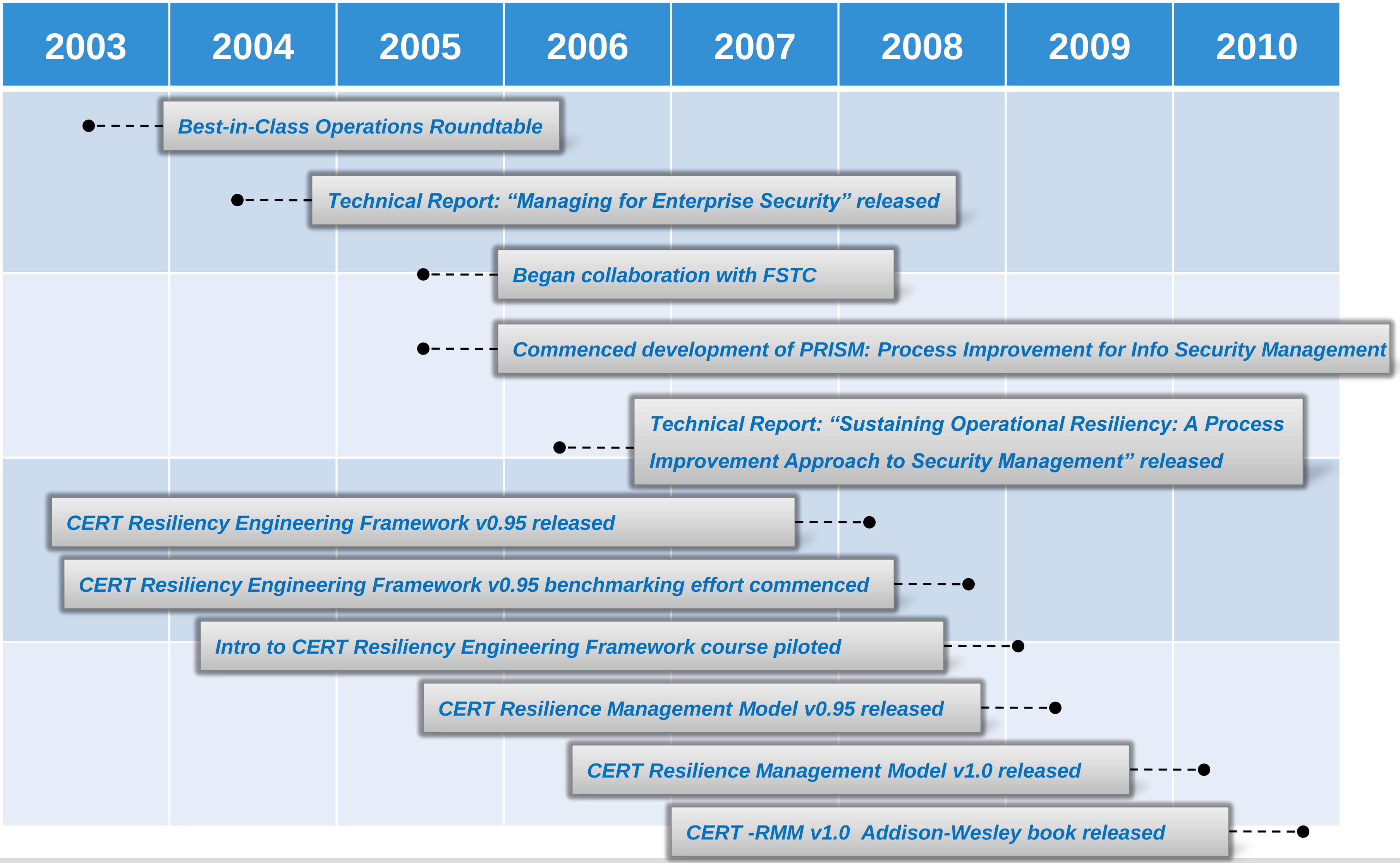
How we got to CERT-RMM version 1.0

CERT-RMM background

CERT-RMM began as research into the application of process improvement and maturity model approaches to security management.

- Literary review and affinity analysis of over 800 standard practices security, BC/DR, and IT ops communities
- Examination of body of knowledge of high-maturity organizations
- Codification of model using trusted CMMI architecture and concepts
- Benchmarking and piloting in the banking/finance community, defense contractors, and US government federal civilian agencies

CERT-RMM timeline



2003 2004 2005 2006 2007 2008 2009 2010

Best-in-Class Operations Roundtable

Technical Report: "Managing for Enterprise Security" released

Began collaboration with FSTC

Commenced development of PRISM: Process Improvement for Info Security Management

Technical Report: "Sustaining Operational Resiliency: A Process Improvement Approach to Security Management" released

CERT Resiliency Engineering Framework v0.95 released

CERT Resiliency Engineering Framework v0.95 benchmarking effort commenced

Intro to CERT Resiliency Engineering Framework course piloted

CERT Resilience Management Model v0.95 released

CERT Resilience Management Model v1.0 released

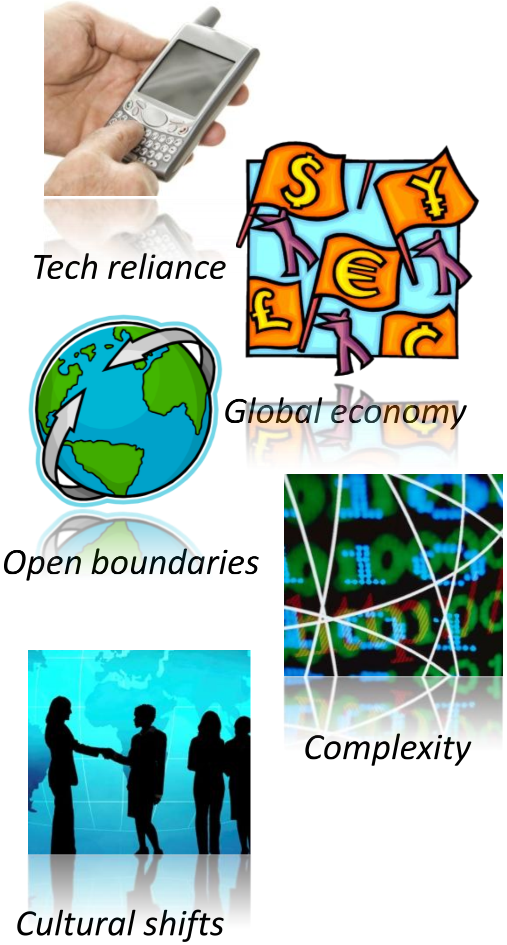
CERT -RMM v1.0 Addison-Wesley book released

© 2010 Carnegie Mellon University

Why CERT-RMM?

The rationale for the model

Imperatives for building CERT-RMM



Increasingly complex operational environments where traditional approaches are failing

Siloed nature of operational risk activities; a lack of convergence

Lack of common language or taxonomy

Overreliance on technical approaches

Lack of means to measure managerial competency

Inability to confidently predict outcomes, behaviors, and performance under times of stress

© 2010 Carnegie Mellon University

Organizational challenges

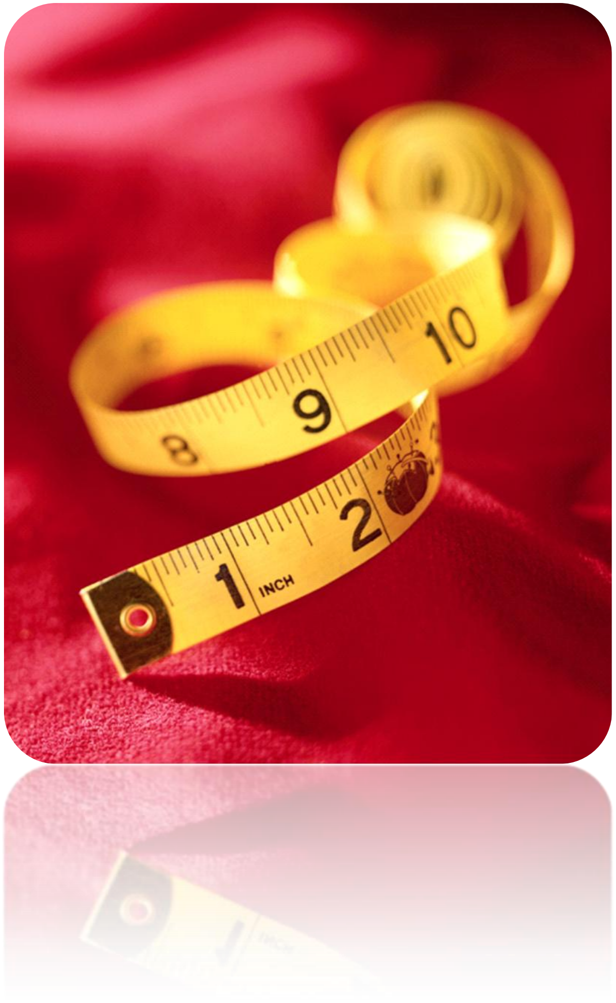
Cope with operational risk and minimize impact

Move all operational risk management activities in the same direction

Optimize cost/effectiveness

Meet mission **no-matter-what**

How do you measure performance before you’re stressed or fail??



© 2010 Carnegie Mellon University

CERT-RMM Building Blocks

Foundational concepts of the model

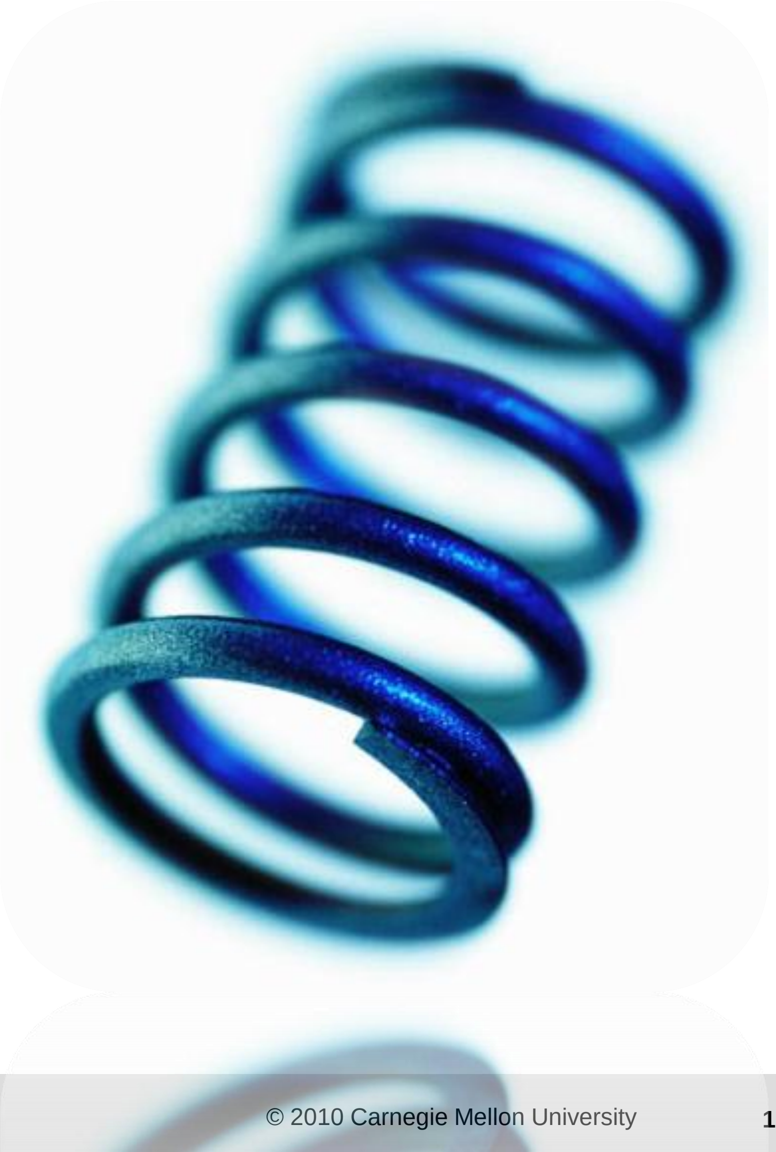
© 2010 Carnegie Mellon University

Operational resilience

Resilience: The physical property of a material when it can return to its original shape or position after deformation that does not exceed its elastic limit [wordnet.princeton.edu]

Operational resilience: The ***emergent*** property of an ***organization*** exhibited when it ***continues to carry out its mission*** after ***disruption*** that ***does not push it beyond*** its ***operational*** limit

[CERT-RMM]



© 2010 Carnegie Mellon University

Operational resilience & operational risk

Security and business continuity are not end-states; they are continuous processes

Effective operational risk management requires harmonization: convergence of these activities working toward the same goals

Operational resilience emerges from effective **operational risk management**

Actions of people

```
A fatal exception
000059F8. The curr

* Press any key to
* Press CTRL+ALT+D
  lose any unsaved
```

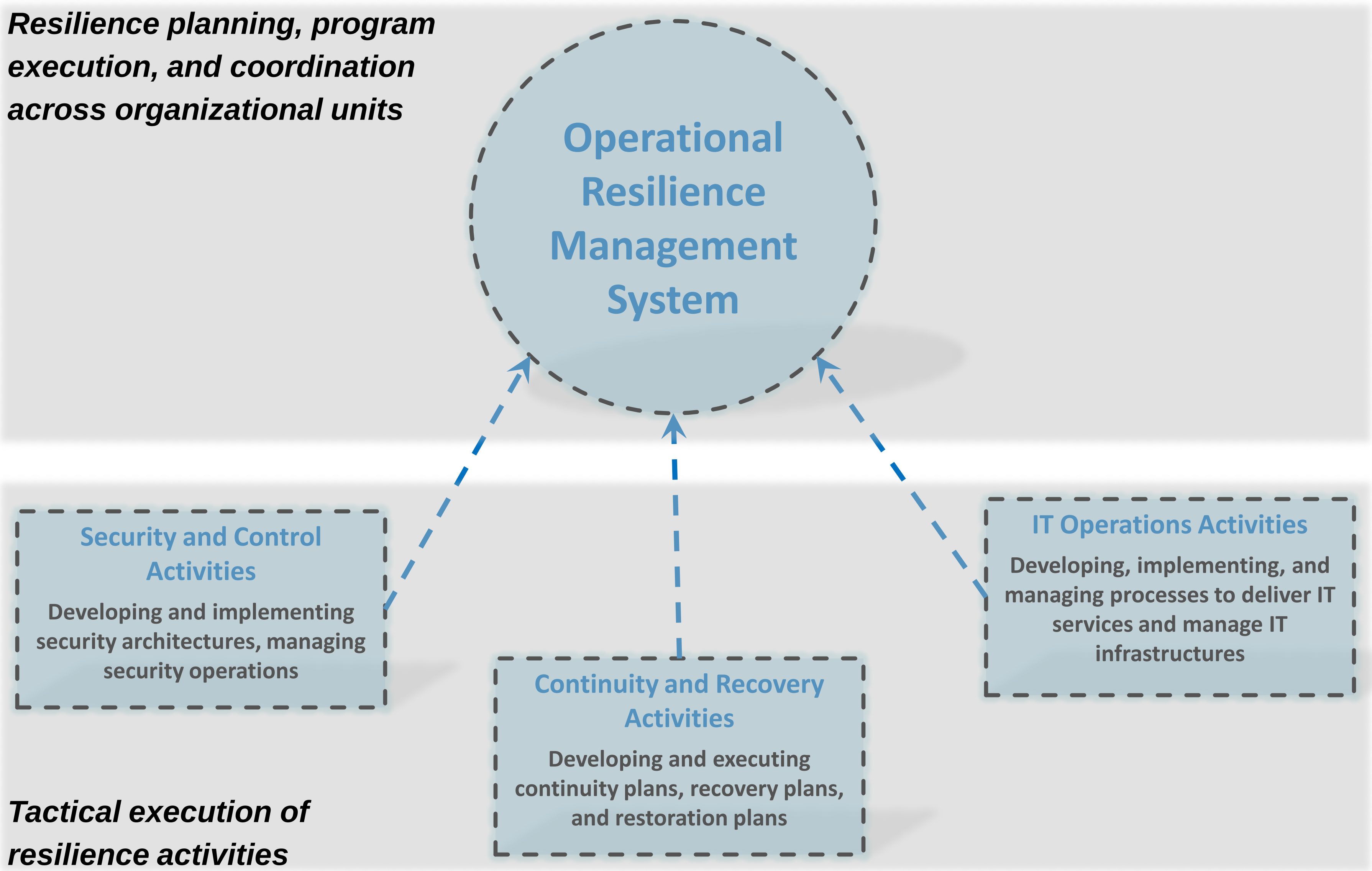
Systems & technology failures

Failed internal processes

External events

© 2010 Carnegie Mellon University

Layers of resilience activities



Resilience planning, program execution, and coordination across organizational units

Operational Resilience Management System

Security and Control Activities

Developing and implementing security architectures, managing security operations

Continuity and Recovery Activities

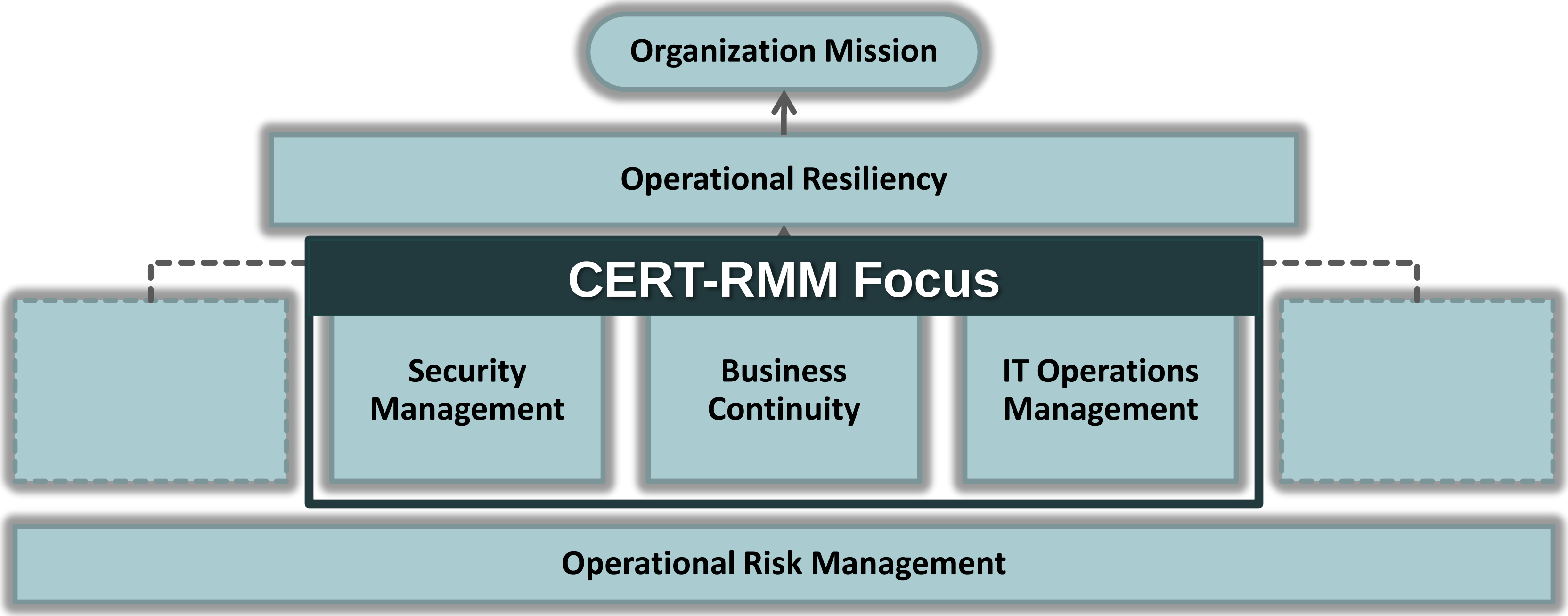
Developing and executing continuity plans, recovery plans, and restoration plans

IT Operations Activities

Developing, implementing, and managing processes to deliver IT services and manage IT infrastructures

Tactical execution of resilience activities

CERT-RMM principle of convergence



Operational resilience is directly affected by convergence

Organizational mission is directly affected by operational resilience

© 2010 Carnegie Mellon University

CERT-RMM foundational elements

Services

The limited number of activities that the organization carries out in performance of a duty or to produce a product

Business Processes

The detailed activities that the organization (and its suppliers) perform to ensure that services meet their mission

Assets

Something of value to the organization required by business processes and services to meet their missions

© 2010 Carnegie Mellon University

Services in CERT-RMM

The organizing concept in CERT-RMM is a **service**

The resilience of **high-value services** in the organization ensures the resilience of the **organization's mission**

Service resilience is a factor of **asset resilience**—if an asset is disrupted or fails, the service may suffer

Service resilience is the object of CERT-RMM processes

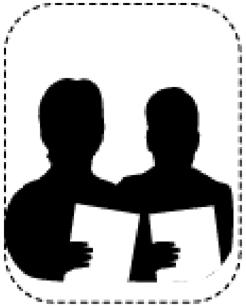
© 2010 Carnegie Mellon University

Assets

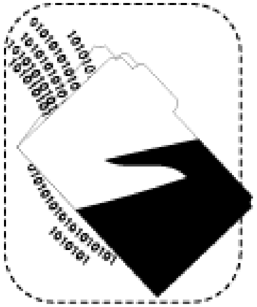
Something of value to the organization

“Charged into production” of business processes and services

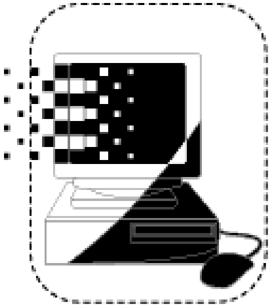
Four types of assets are the focus of operational resilience management as defined in CERT-RMM.



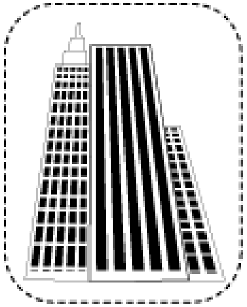
people



information



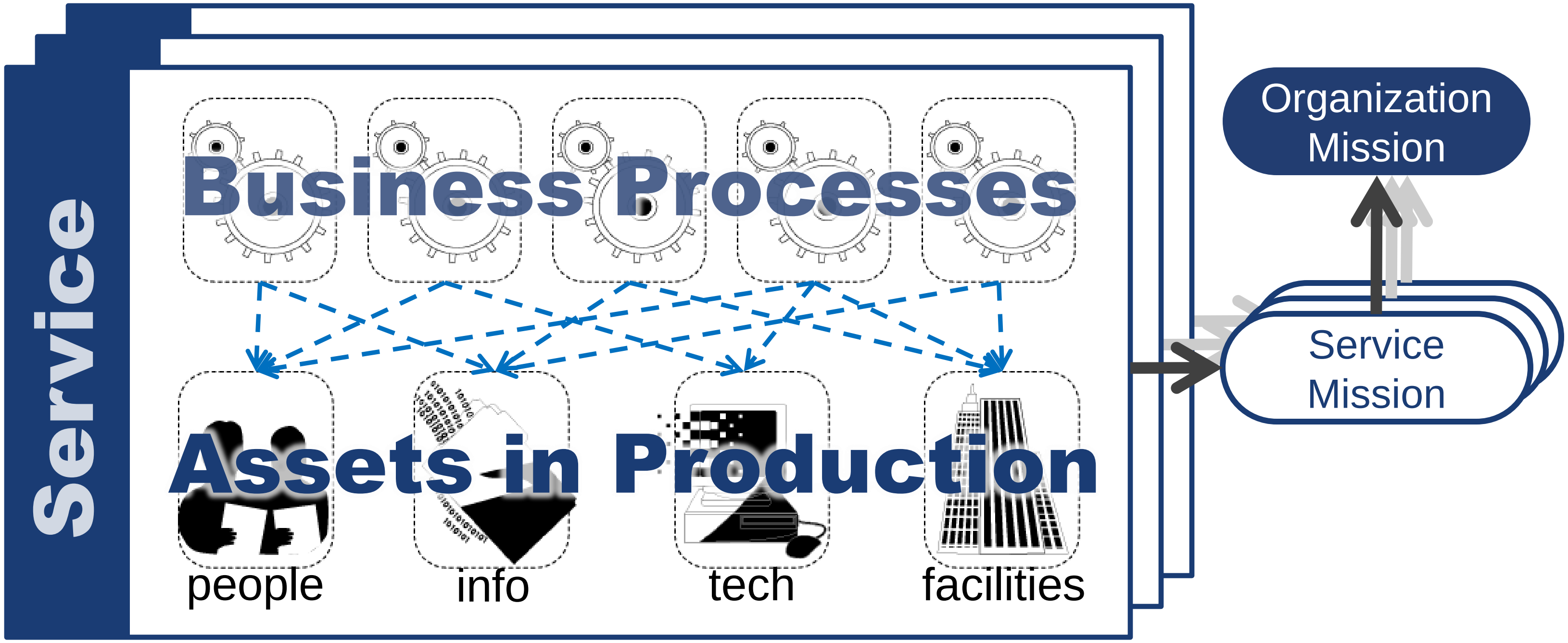
technology



facilities

© 2010 Carnegie Mellon University

Assets charged into production



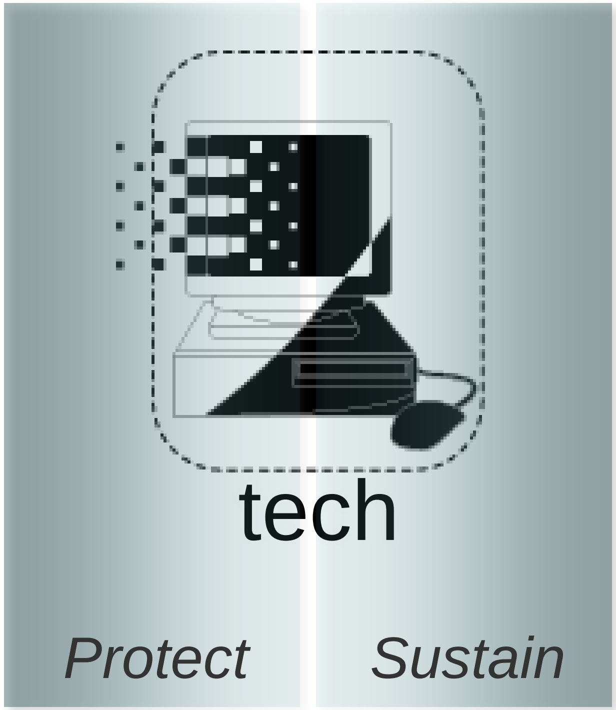
Asset value relates to the importance of the **asset** in meeting the **business process** and **service** mission.

Operational resilience starts at the asset level

To ensure operational resilience at the **service level**, related assets must be

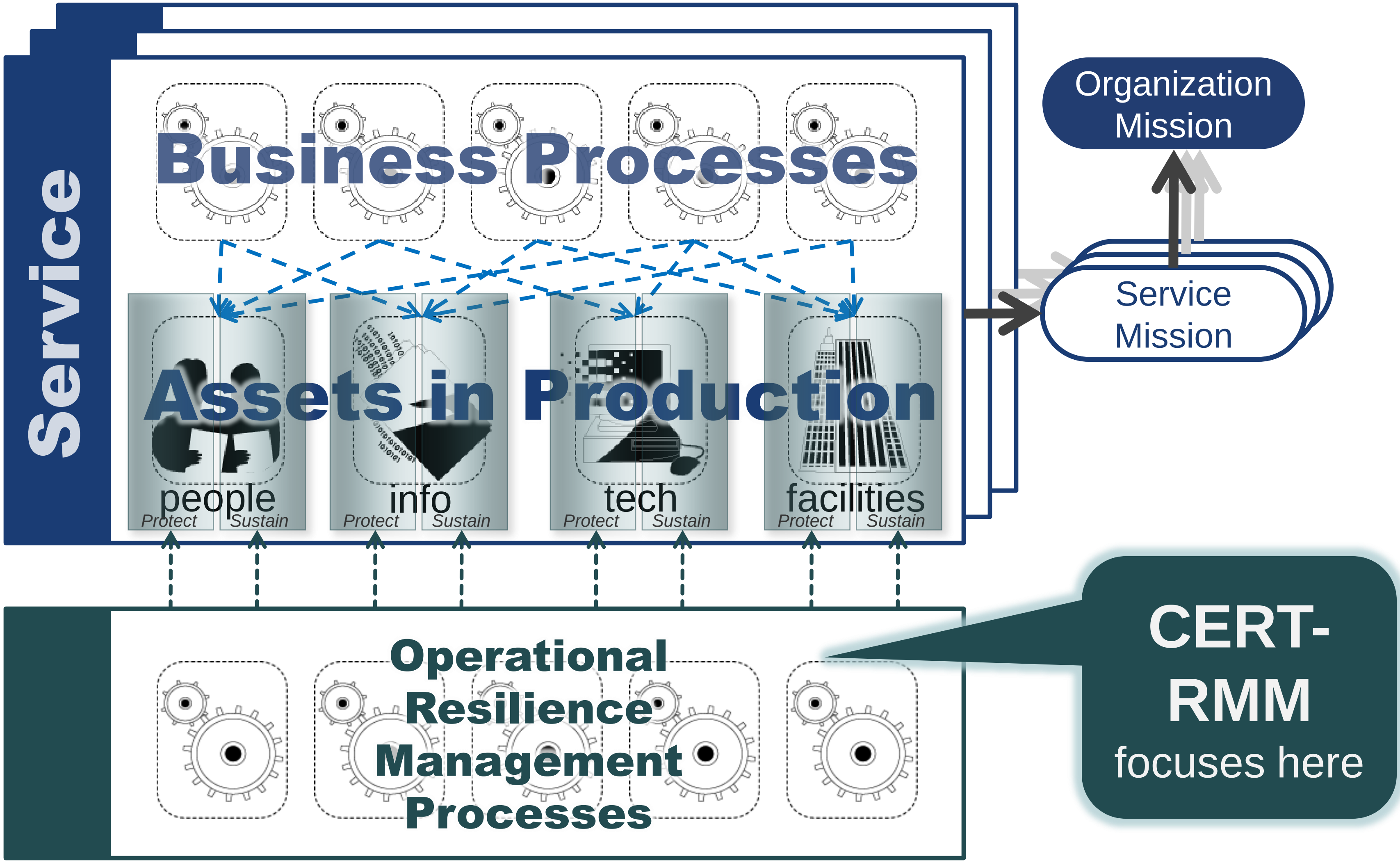
- Protected from threats and risks that could disable them
- Made sustainable under adverse conditions

The optimal “mix” of these strategies depends on the **value of the asset** and the **cost of deploying and maintaining the strategy.**



© 2010 Carnegie Mellon University

Organizational context for resilience activities



CERT-RMM focuses here

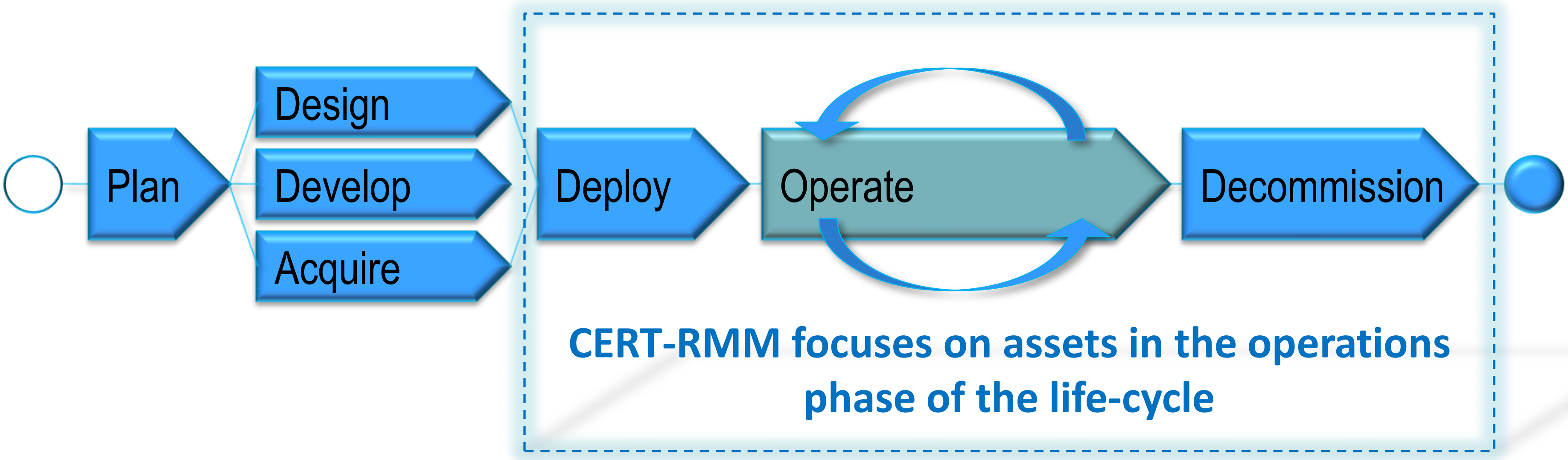
© 2010 Carnegie Mellon University

CERT-RMM Architecture

Foundational structures on which the model is built

CERT-RMM in the life-cycle

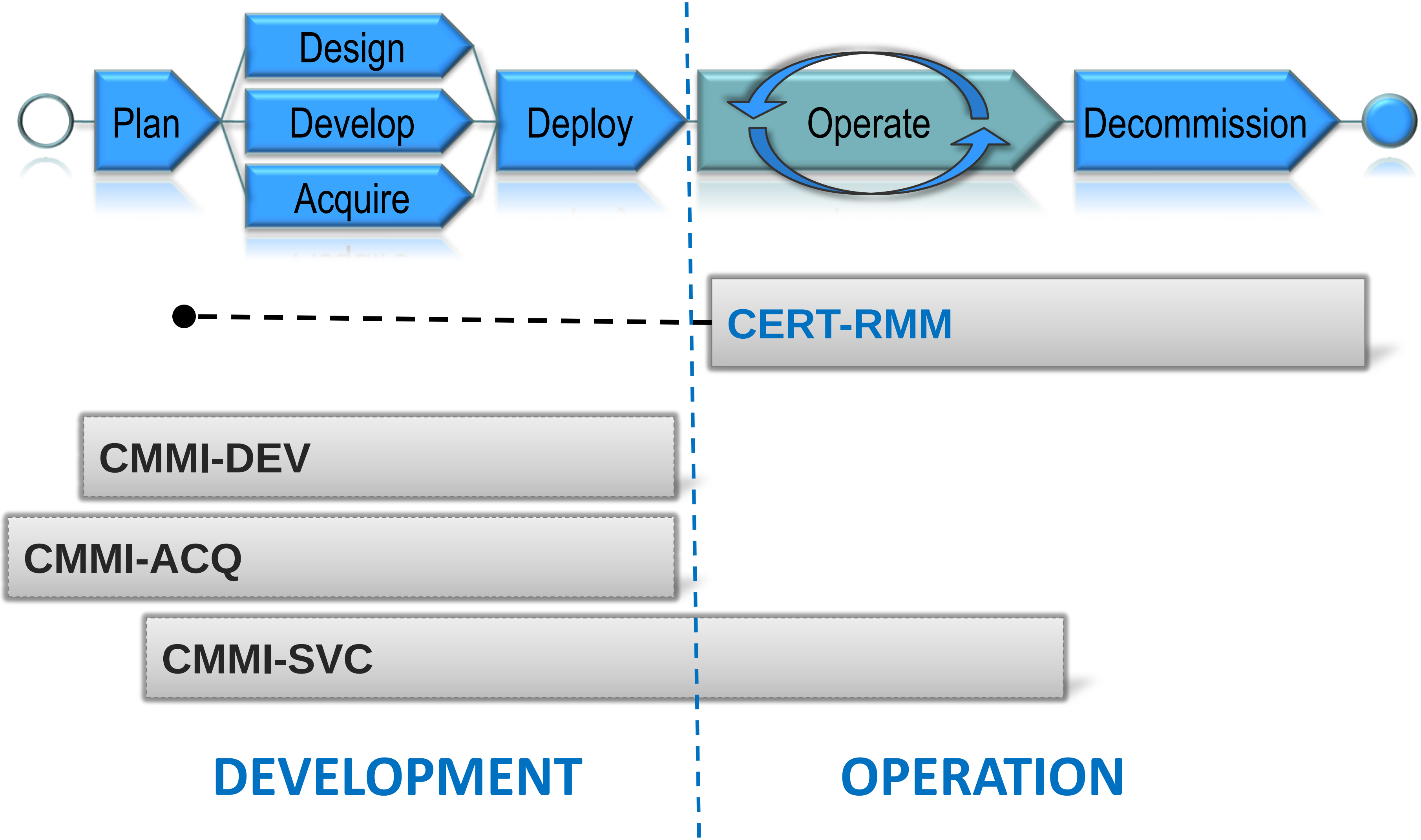
Operational resilience management focuses on the deploy, operate, and decommission phases, but reaches back to development phase of lifecycle to ensure consideration of security and continuity issues prior to placing assets in production.



CERT-RMM focuses on assets in the operations phase of the life-cycle

© 2010 Carnegie Mellon University

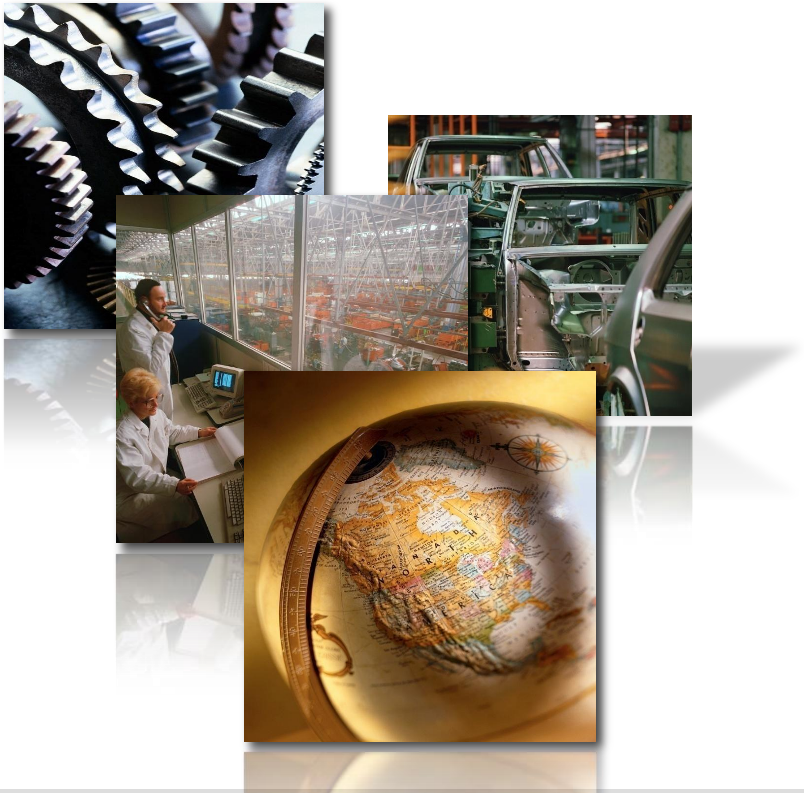
For comparison: CERT-RMM & CMMI



© 2010 Carnegie Mellon University

CERT-RMM architectural elements

CERT-RMM uses proven architectural elements of CMMI and applies them in an operational context.



- 26 **process areas**
- Arranged in a **continuous representation**
- Goals, practices, sub-practices, and work products that *specifically* define each process area
- Goals, practices, and sub-practices that *generically* define increasing levels of capability
- Implementation and adoption examples
- An **appraisal methodology** to determine capability levels

© 2010 Carnegie Mellon University

CERT-RMM at a glance

Engineering	
ADM	Asset Definition and Management
CTRL	Controls Management
RRD	Resilience Requirements Development
RRM	Resilience Requirements Management
RTSE	Resilient Technical Solution Engineering
SC	Service Continuity

Enterprise Management	
COMM	Communications
COMP	Compliance
EF	Enterprise Focus
FRM	Financial Resource Management
HRM	Human Resource Management
OTA	Organizational Training & Awareness
RISK	Risk Management

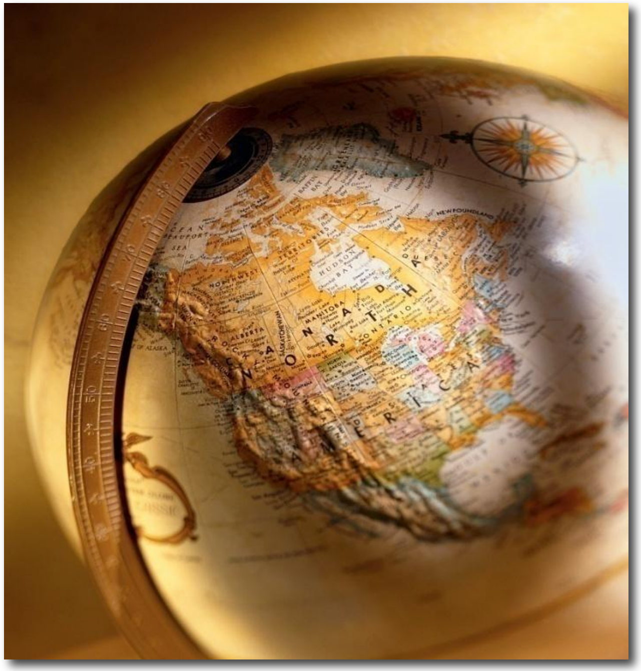
Operations Management	
AM	Access Management
EC	Environmental Control
EXD	External Dependencies
ID	Identity Management
IMC	Incident Management & Control
KIM	Knowledge & Information Management
PM	People Management
TM	Technology Management
VAR	Vulnerability Analysis & Resolution

Process Management	
MA	Measurement and Analysis
MON	Monitoring
OPD	Organizational Process Definition
OPF	Organizational Process Focus

26 Process Areas in 4 categories

Enterprise management

Seven process areas that support the resilience management process



Governance, Risk, & Compliance

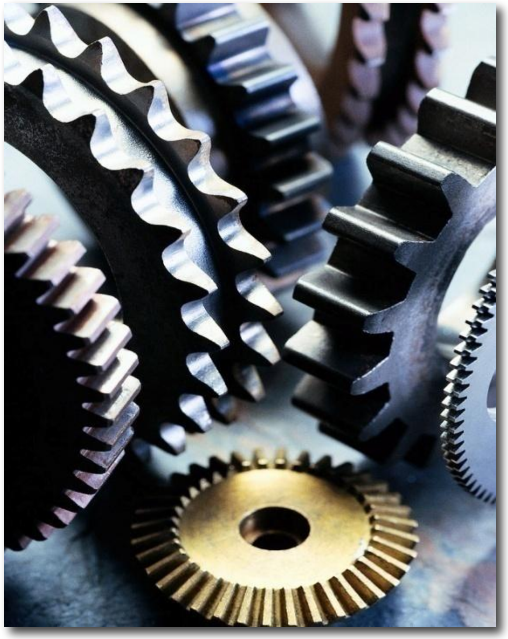
COMP EF RISK

Supporting Resilience

COMM FRM HRM OTA

Engineering

Six process areas for establishing resilience for organizational assets, business processes, and services



Asset Management

ADM

Requirements Management

RRD RRM

Establishing and Managing Resilience

CTRL RTSE SC

Operations management

Nine process areas for managing the operational aspects of resilience

Asset Resilience Management

EC KIM PM TM

Threat, Incident, & Access Management

AM ID IMC VAR

Supplier Management

EXD

© 2010 Carnegie Mellon University

Process management process areas

Four process areas for defining, planning, deploying, implementing, monitoring, controlling, appraising, measuring, and improving operational resilience management processes

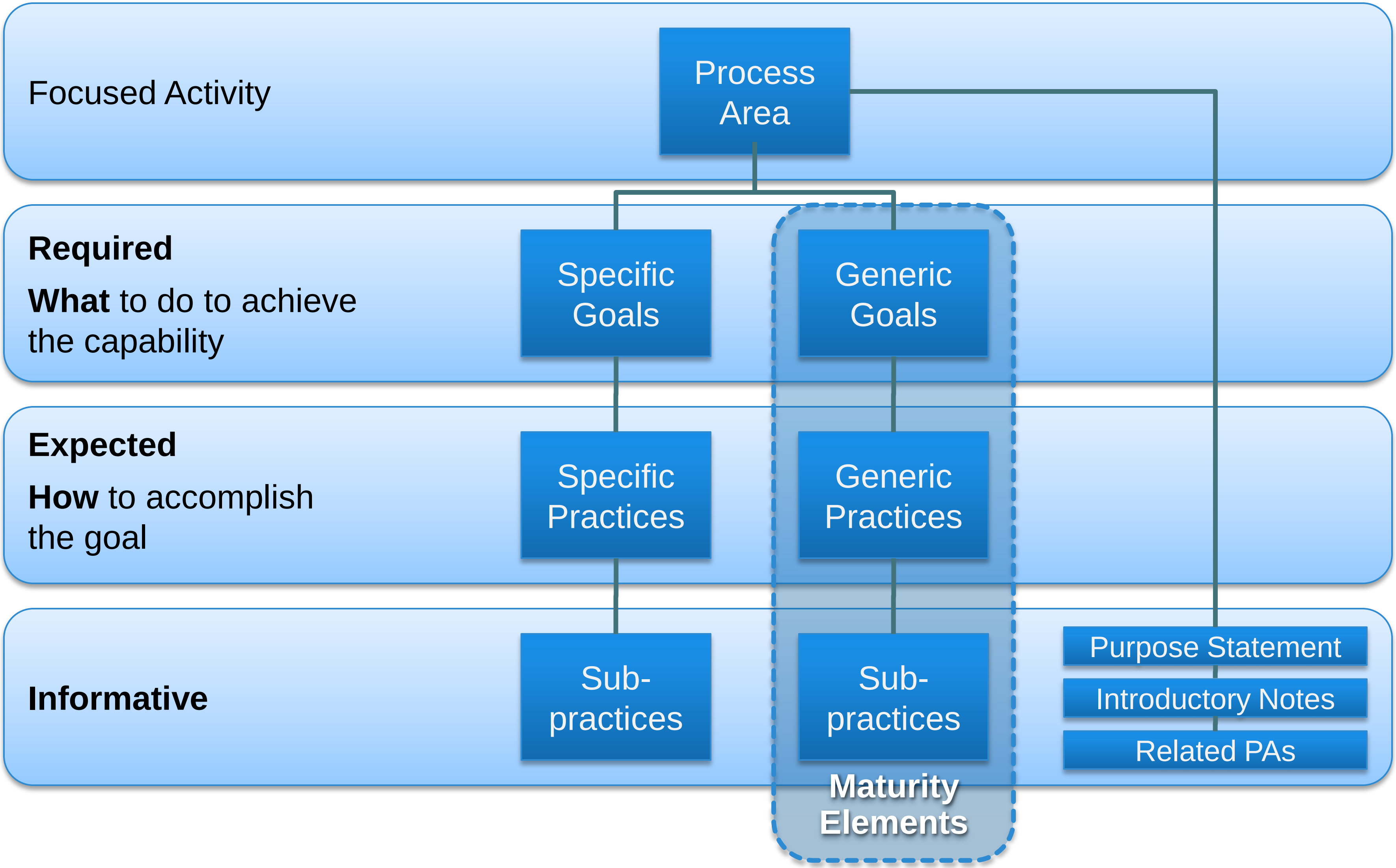
Data Collection & Logging

MON

Process Management

MA OPD OPF

CERT-RMM process area structure



Focused Activity

Process Area

Required

What to do to achieve the capability

Specific Goals

Generic Goals

Expected

How to accomplish the goal

Specific Practices

Generic Practices

Informative

Sub-practices

Sub-practices

Purpose Statement

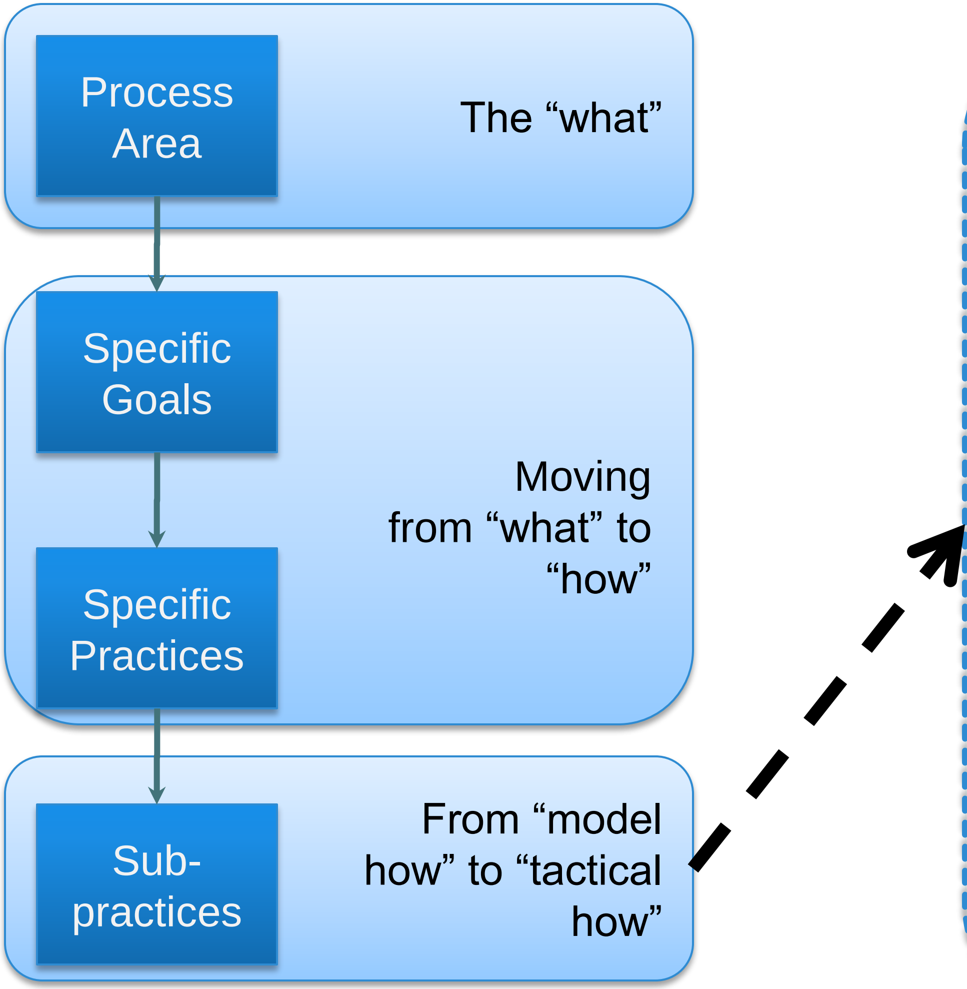
Introductory Notes

Related PAs

Maturity Elements

© 2010 Carnegie Mellon University

CERT-RMM links to codes of practice



Codes of Practice:

- BS25999-1:2006
- CMMI v1.2
- CMMI for Services
- CobiT 4.1
- COSO ERM
- DRII GAP
- FFIEC Handbooks (Security, BCP)
- ISO 20000-1:2005(E)
- ISO 20000-2:2005(E)
- ISO 24762:2008(E)
- ISO 27001:2005
- NFPA 1600 (2007)
- PCI DSS v1.1
- Val-IT

© 2010 Carnegie Mellon University

The Capability Dimension of CERT-RMM

Measuring process institutionalization to determine capability under stress

© 2010 Carnegie Mellon University

The promise of process institutionalization

The “capability” dimension of CERT-RMM sets it apart from other models in the operational resilience space

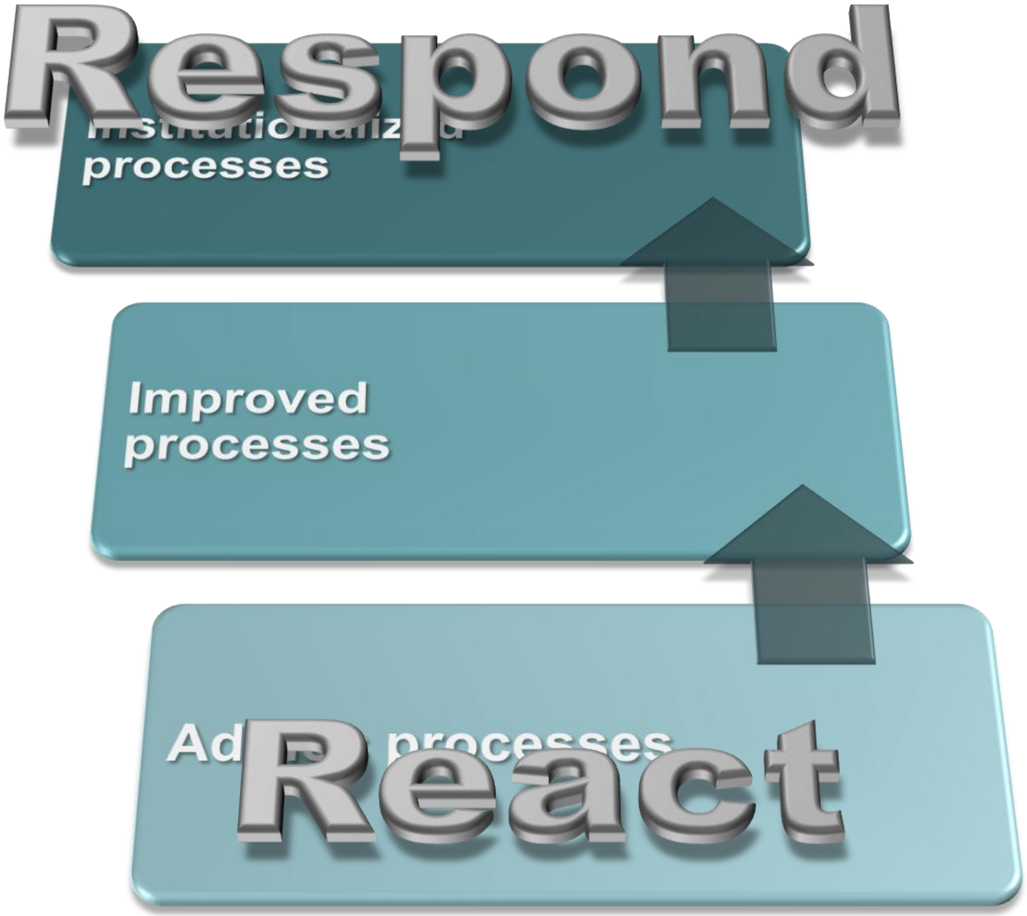
“Capability” determines the degree to which

- A process has been ingrained in the way that work is defined, executed, and managed
- There is commitment and consistency to performing the process

Measuring capability helps you determine the degree to which you are able to control the output of the process—in this case, the degree to which you can predict how well you’ll perform under times of stress

© 2010 Carnegie Mellon University

Process institutionalization



Higher degrees of process institutionalization should translate to more stable processes that

- produce consistent results over time
- are retained during times of stress

© 2010 Carnegie Mellon University

Value of knowing your “capability” level

The degree of process institutionalization can help to answer several important questions in managing operational resilience:

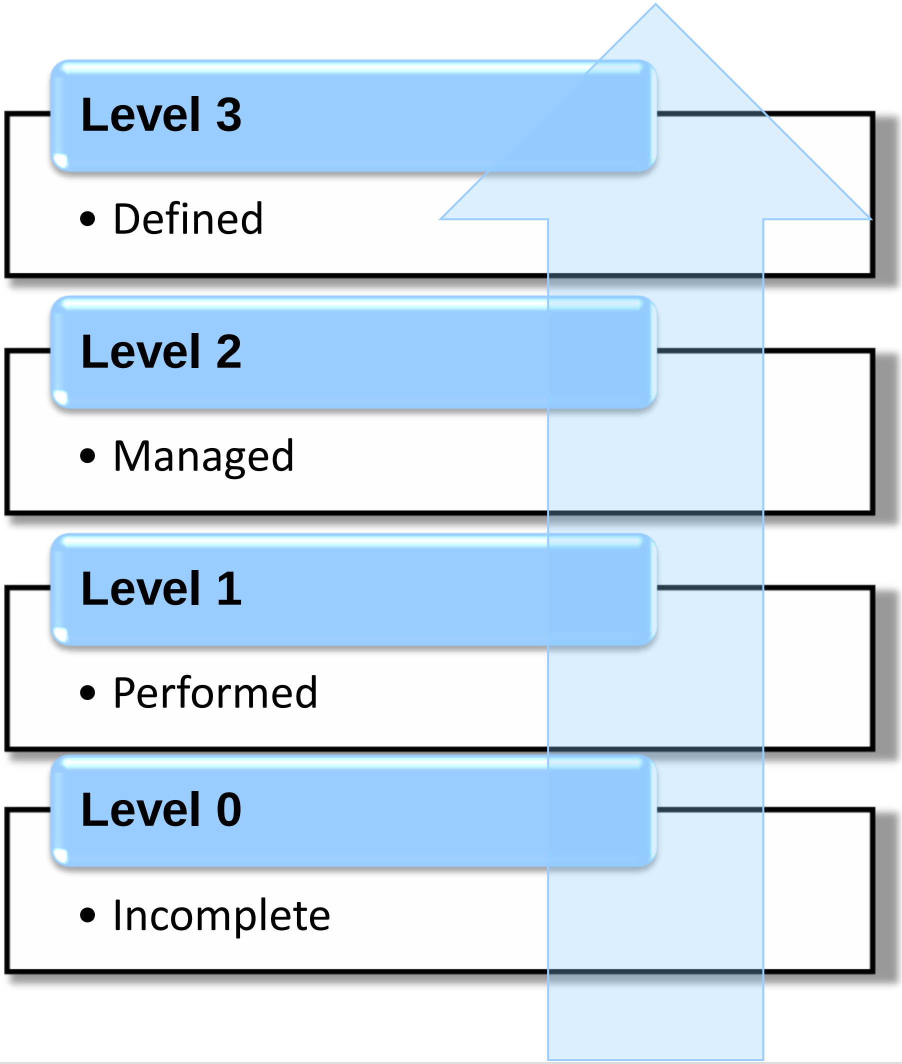
- How well are we performing today?
- Can we repeat our successes?
- Do we consistently produce expected results?
- Can we adapt seamlessly to changing risk environments?
- Are our processes stable enough to depend on them under times of stress?
- Can we predict how we will perform under times of stress?

You need to know not only that you’re doing the right things but that you are doing them in a sustainable way.

© 2010 Carnegie Mellon University

Process institutionalization in CERT-RMM

Capability levels are used in CERT-RMM to represent process institutionalization



Level 3

- Defined

Level 2

- Managed

Level 1

- Performed

Level 0

- Incomplete

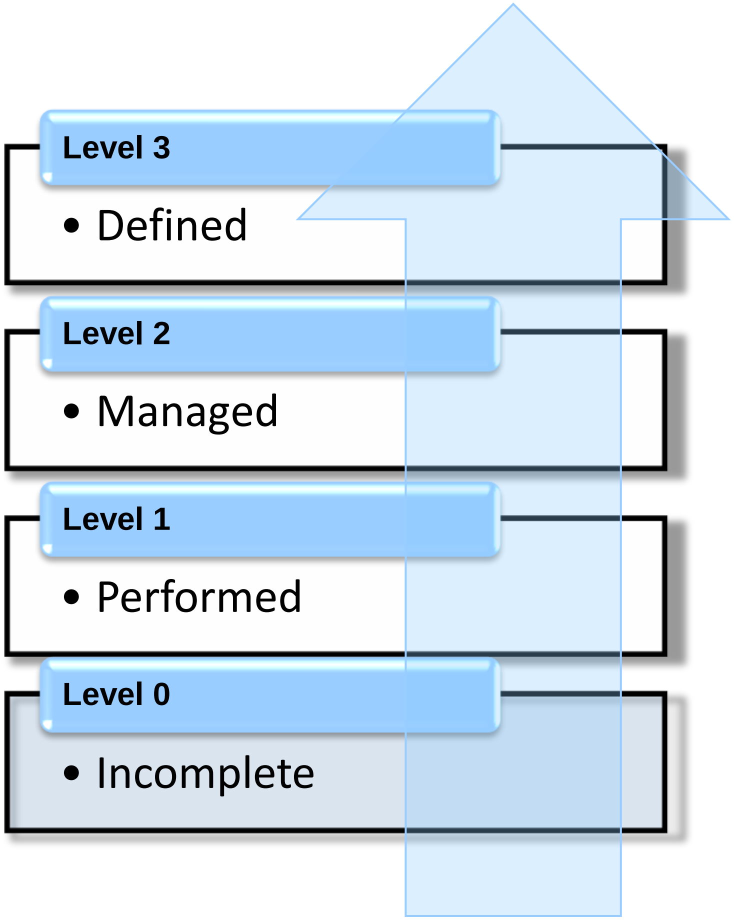
Processes are acculturated, defined, measured, and governed

Practices are performed

Practices are incomplete

© 2010 Carnegie Mellon University

Level 0 - Incomplete

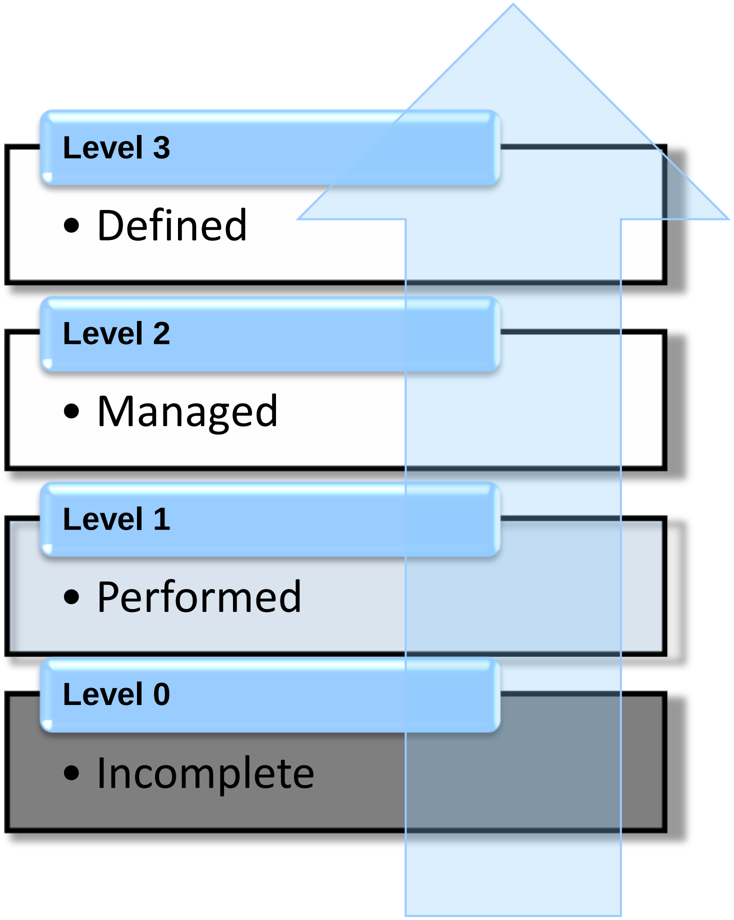


Indicates that one or more of the specific goals of the process area is not being achieved

Represents an incomplete process, therefore cannot be institutionalized

© 2010 Carnegie Mellon University

Level 1 - Performed



Represents a **performed** process

Satisfies the specific goals of the process area

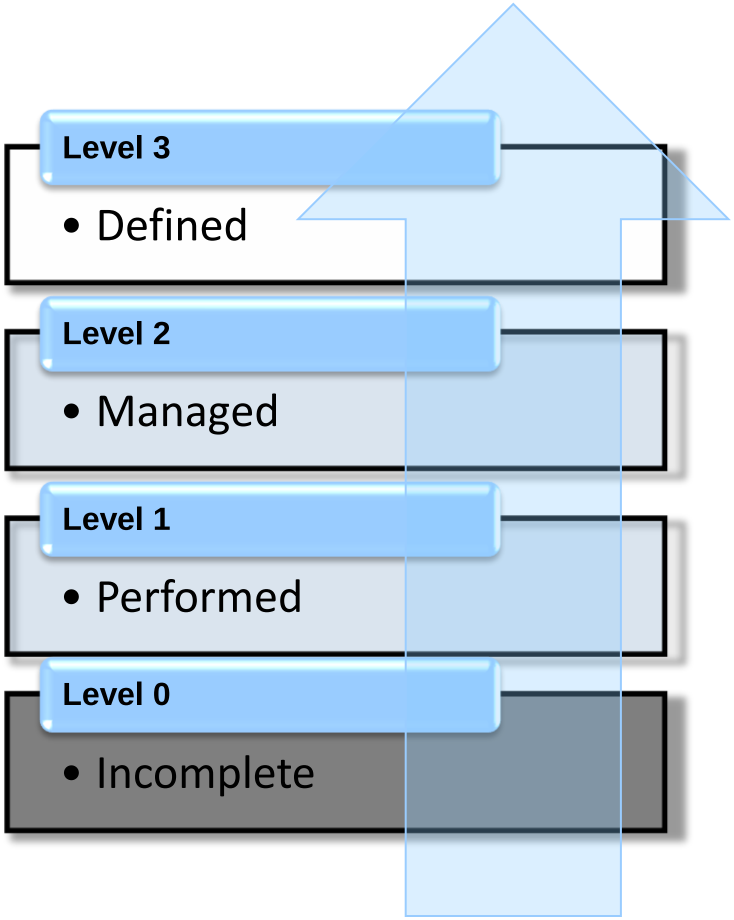
Supports and enables the work needed to produce the expected process work products

Provides improvement, but can be lost over time without institutionalization

Improvements can only be maintained and sustained by moving to higher capability levels (i.e., levels 2 and beyond).

© 2010 Carnegie Mellon University

Level 2 - Managed



Represents a **performed** process that has the basic infrastructure in place to support the process

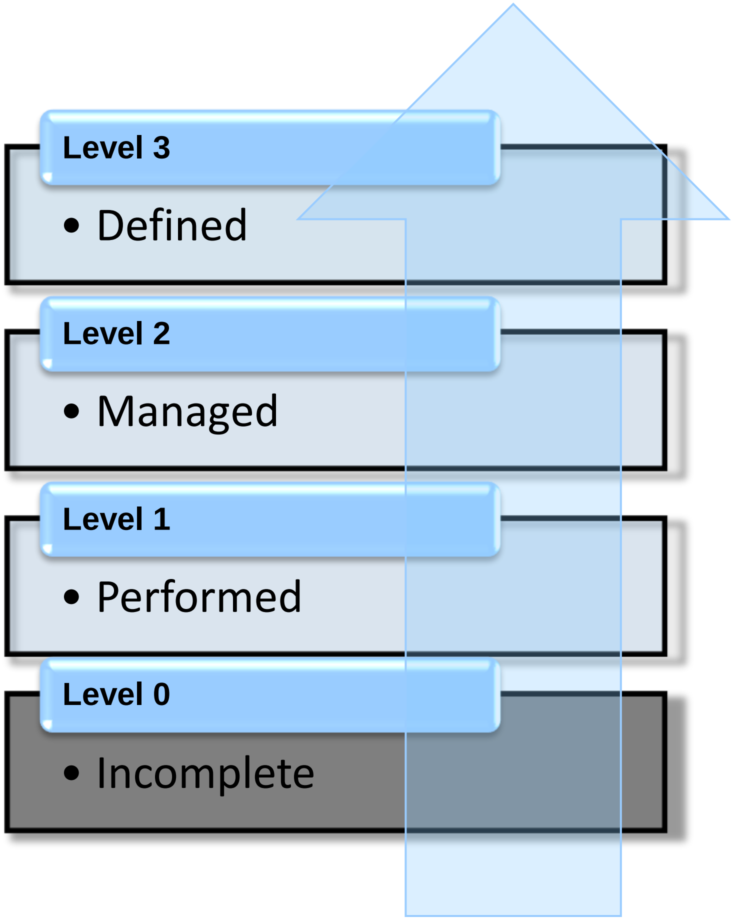
The process is:

- Governed
- Planned and executed in accordance with policy
- Employs skilled people who have adequate resources
- Involves relevant stakeholders
- Is monitored, controlled, and reviewed
- Is evaluated for adherence to its process description

Process discipline ensures that existing practices are retained during times of stress.

© 2010 Carnegie Mellon University

Level 3 - Defined



Represents a **managed** process that is tailored from the organization's set of standard processes

Contributes work products, measures, and other process improvement information to the organizational process assets

Scope difference from level 2—provides consistency of process assets across organizational units

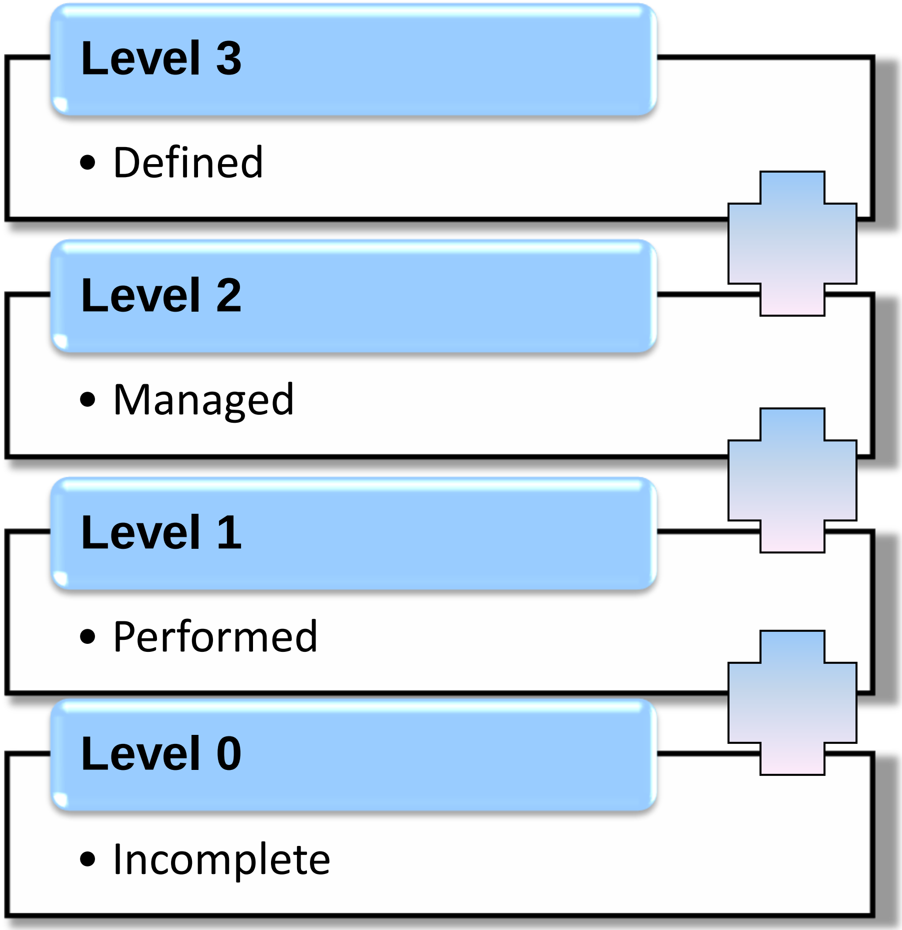
More rigorous description of processes

Process management is proactive, not reactive

Highly important in RMM—because of the "enterprise" and convergence orientation

© 2010 Carnegie Mellon University

Capability levels are cumulative



Achieving Level 3 means achieving (and sustaining) Level 1 (specific goals) plus Level 2 and Level 3 generic goals, and so on. . .

Example: Asset Definition & Management

Specific Goals	Specific Practices
ADM:SG1 Establish Organizational Assets	ADM:SG1.SP1 Inventory Assets
	ADM:SG1.SP2 Establish a Common Understanding
	ADM:SG1.SP3 Establish Ownership and Custodianship
ADM:SG2 Establish Relationship Between Assets and Services	ADM:SG2.SP1 Associate Assets with Services
	ADM:SG2.SP2 Analyze Asset-Service Dependencies
ADM:SG3 Manage Assets	ADM:SG3.SP1 Identify Change Criteria
	ADM:SG3.SP2 Maintain Changes to Assets and Inventory

© 2010 Carnegie Mellon University

Institutionalizing *Asset Definition & Management*

Specific Goals	Specific Practices
ADM:SG1 Establish Organizational Assets	ADM:SG1.SP1 Inventory Assets
	ADM:SG1.SP2 Establish a Common Understanding
	ADM:SG1.SP3 Establish Ownership and Custodianship
ADM:SG2 Establish Relationship Between Assets and Services	ADM:SG2.SP1 Associate Assets with Services
	ADM:SG2.SP2 Analyze Asset-Service Dependencies
ADM:SG3 Manage Assets	ADM:SG3.SP1 Identify Change Criteria
	ADM:SG3.SP2 Maintain Changes to Assets and Inventory

A **managed** process is:

- Governed
- Executed according to policy
- Employs skilled people
- Involves relevant stakeholders
- Monitored, controlled, and reviewed
- Evaluated for adherence to the organization’s process description
- Regularly reviewed with senior management

Practice example: *ADM.SG1.SP1-Inventory Assets*

To institutionalize the performance of the “Inventory Assets” practice, you must commit to and perform these supporting practices:

Institutionalizing Factor	Institutionalizing Practice
Governed	There is a policy requiring periodic asset inventory activities; the activity has oversight and corrective actions are taken when necessary
Employs skilled people	Staff involved in the practice have the appropriate skill levels and training
Involves stakeholders	Asset owners and custodians are involved; all involved in protecting and sustaining the asset are involved
Monitored and controlled	The process is measured to determine effectiveness. Examples: % of assets inventoried; # of changes to inventory in a given period
Evaluate adherence	The process as performed is verified to be aligned with the process definition
Review with senior management	Keep management informed on the results of the process and identify and resolve issues

© 2010 Carnegie Mellon University

Determining Capability using CERT-RMM

Determining an organization's capability for managing operational resilience

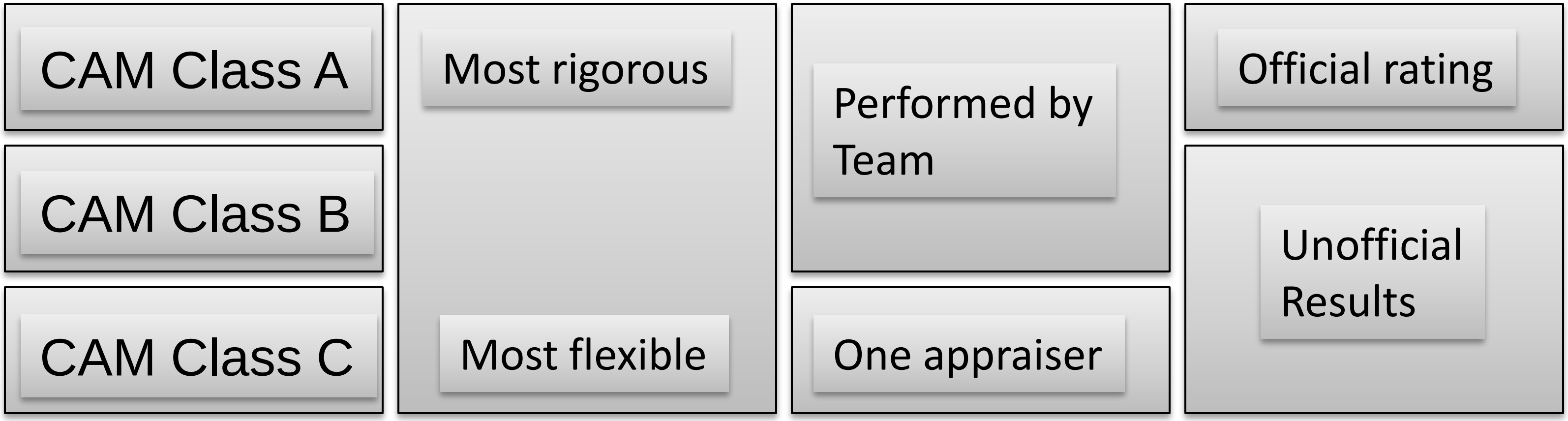
© 2010 Carnegie Mellon University

CERT-RMM capability appraisals

An appraisal is used to evaluate (or diagnose) the organization using CERT-RMM as the basis.

The SCAMPI^{SM} appraisal method from SEI forms the foundation of the CERT-RMM Capability Appraisal Method (RMM CAM)

There are three classes of CERT-RMM appraisals:



CAM Class A

CAM Class B

CAM Class C

Most rigorous

Most flexible

Performed by Team

One appraiser

Official rating

Unofficial Results

CERT-RMM capability survey

A self-directed assessment instrument that provides a quick organizational “health check”

Low investment, but potentially high impact

Can be used to catalyze a more formal process improvement effort

Currently in development; to be released by year-end 2010

Not considered to be one of the “class” appraisals and not based on the SCAMPI method

Value of a CERT-RMM appraisal

Process improvement model can allow for third-party appraisals

Creation of a set of professionals skilled in rating process performance

Elimination of subjectivity in rating process performance and institutionalization

Ability to provide statistics on organization and industry capability levels

© 2010 Carnegie Mellon University

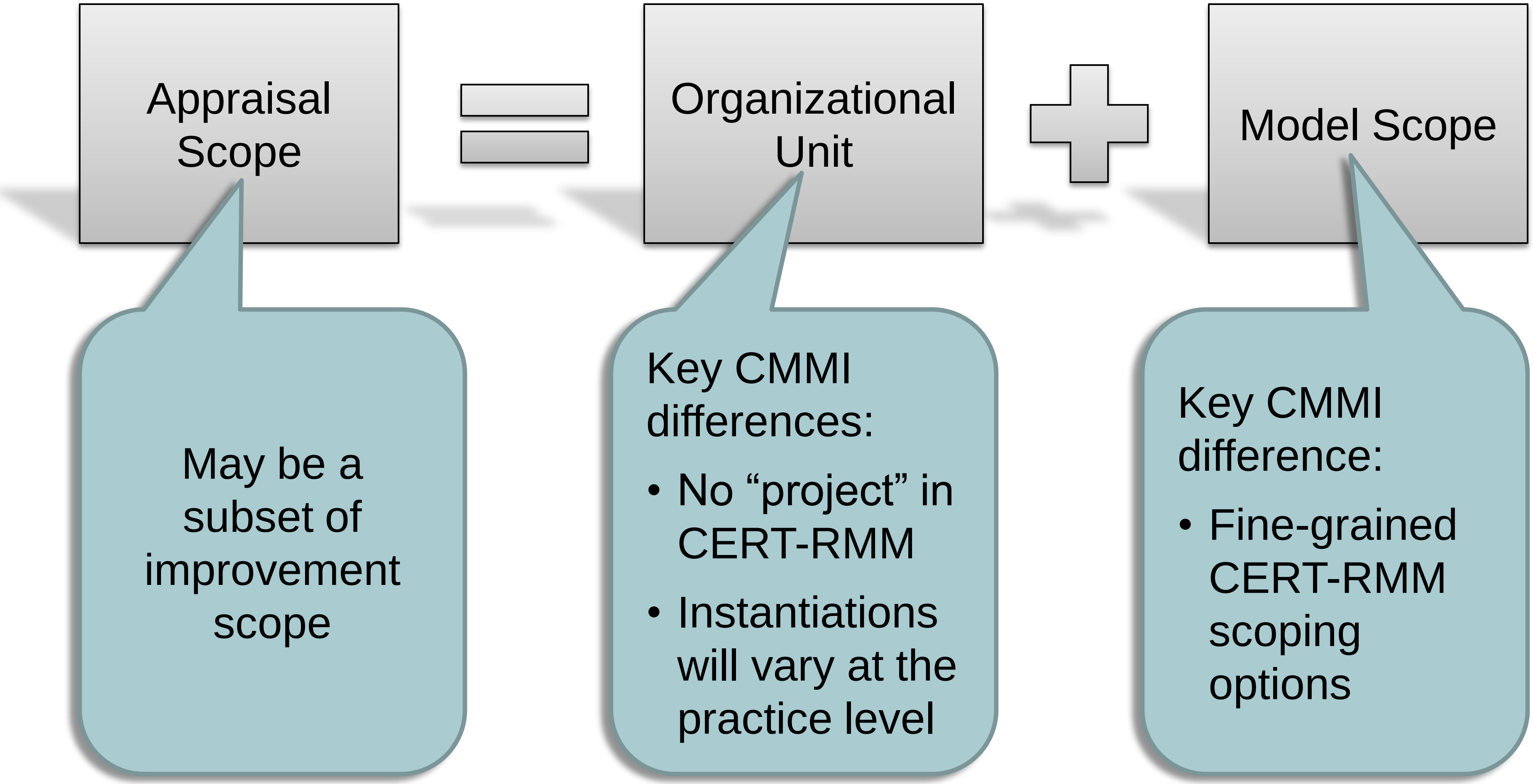
Appraisal scope

The depth of the CERT-RMM appraisal can vary depending on the organization’s objectives. (i.e., It can simply help the organization to determine where it is or it can lead to a formal capability level rating.)

Can include one process area or a group of process areas

- Can be broad:
  - One process area over many operational units
- Or deep:
  - Many process areas in one operational unit

Appraisal scope



Appraisal Scope

Organizational Unit

Model Scope

May be a subset of improvement scope

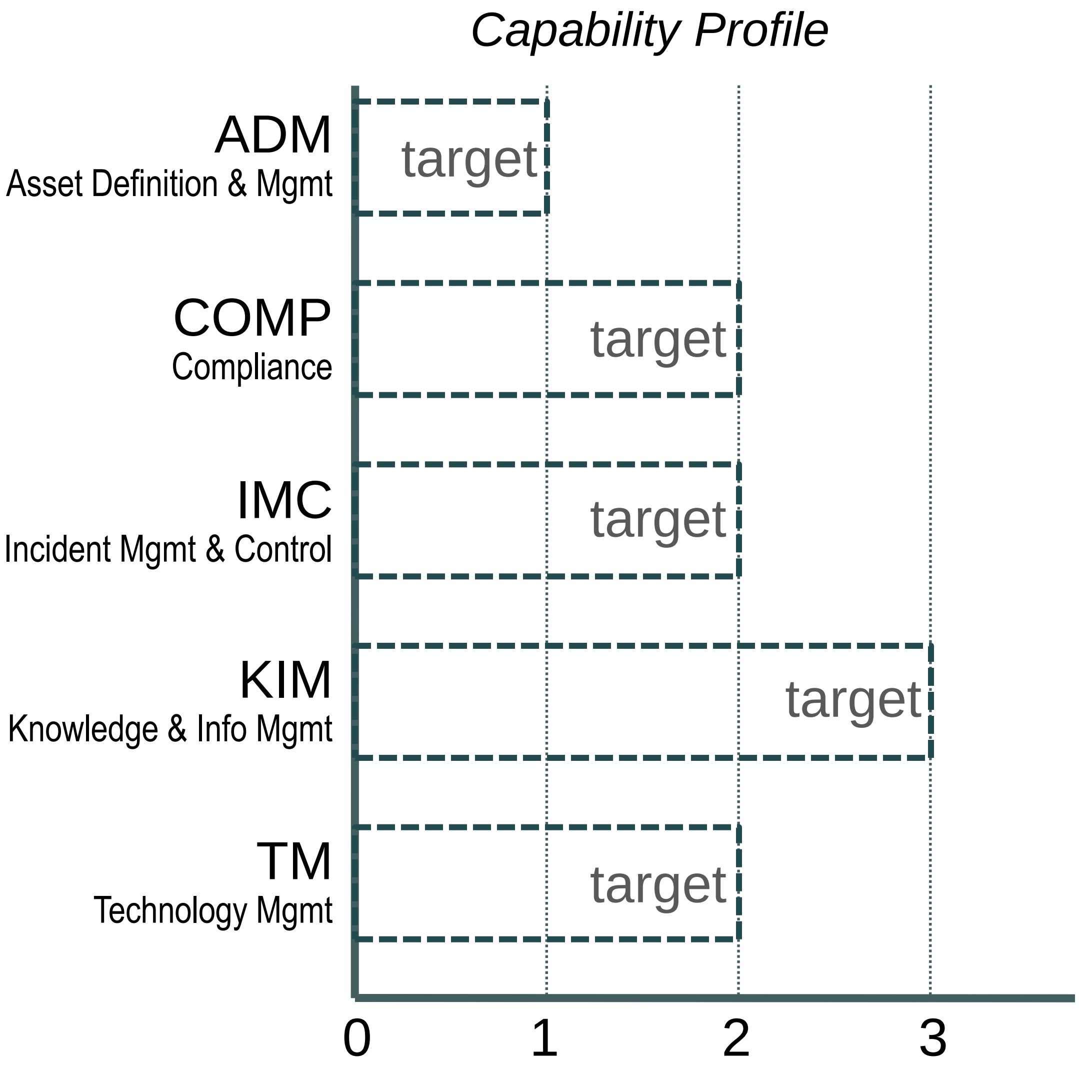
Key CMMI differences:

- No “project” in CERT-RMM
- Instantiations will vary at the practice level

Key CMMI difference:

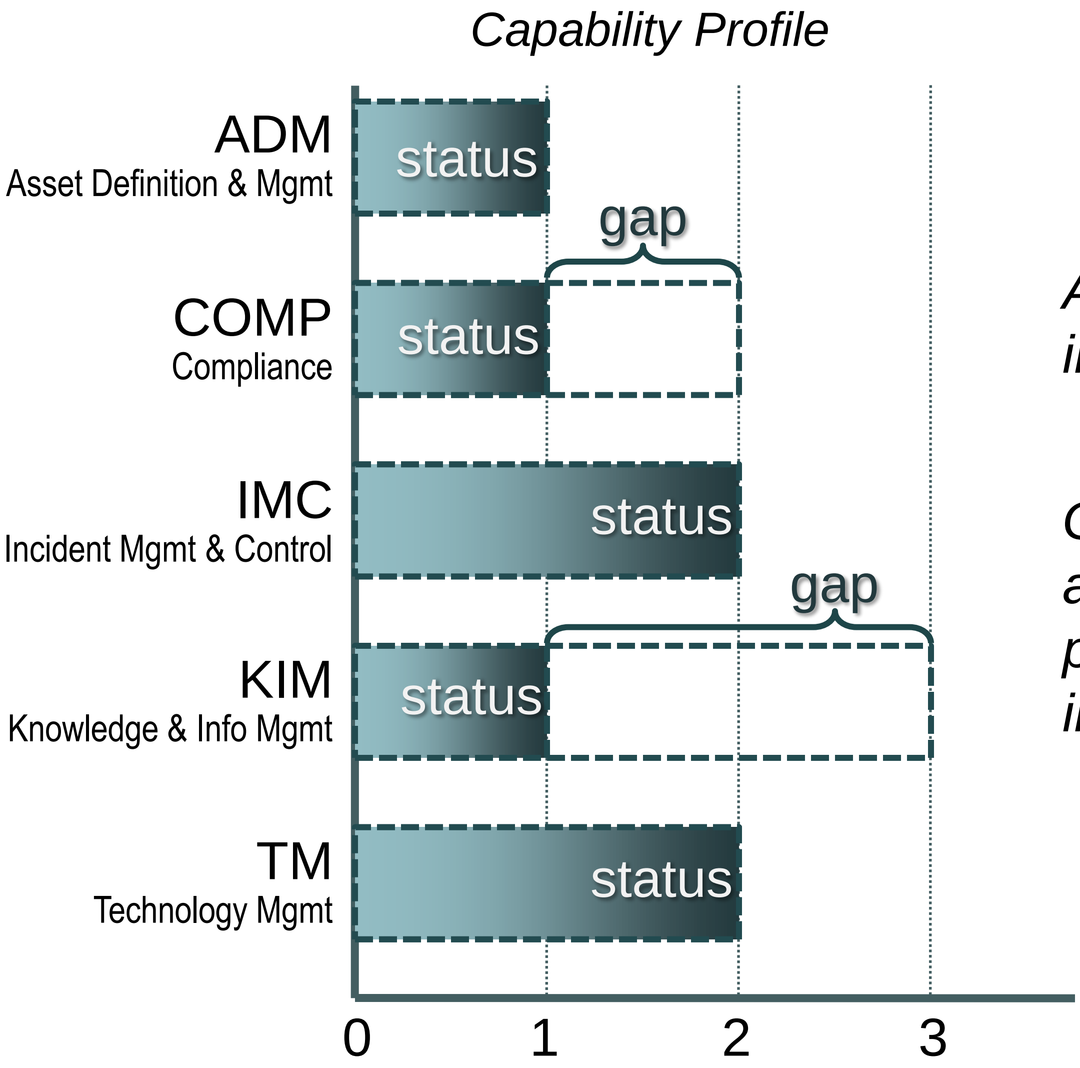
- Fine-grained CERT-RMM scoping options

Appraisal scope: capability profile



© 2010 Carnegie Mellon University

Appraisal results



Appraisal results may indicate gaps

Gaps should be analyzed and prioritized prior to implementing improvements

© 2010 Carnegie Mellon University

CERT-RMM Credentialing

Certifying CERT-RMM professionals

© 2010 Carnegie Mellon University

CERT-RMM professional roles

CERT-RMM Appraiser

CERT-RMM Navigator

CERT-RMM Coach

CERT-RMM Appraisal Team Member

These roles are under development—priority will be based on demand

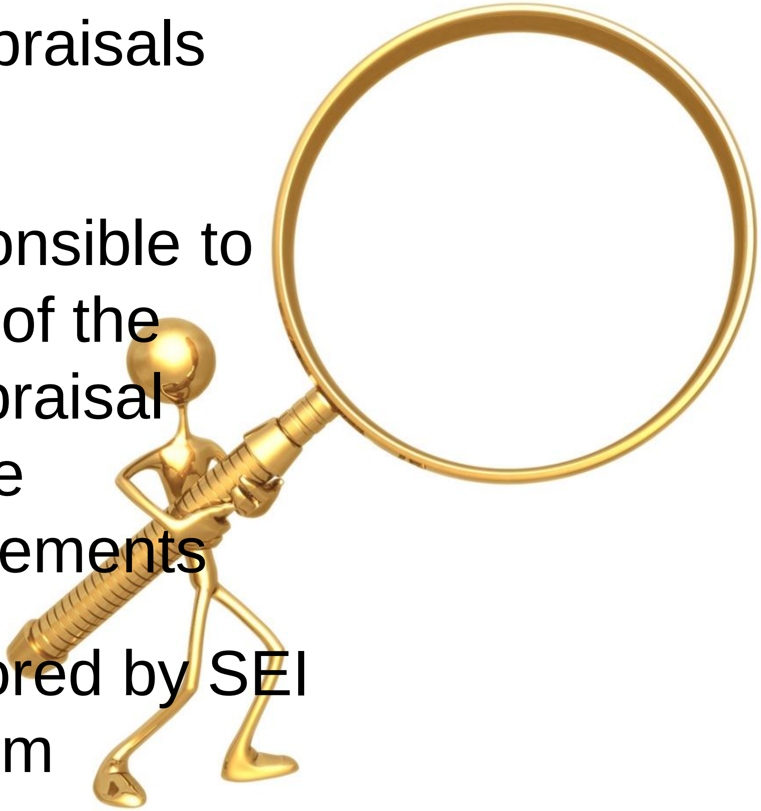
© 2010 Carnegie Mellon University

CERT-RMM Appraiser

SEI-Certified CERT-RMM Appraisers can lead all classes (A, B, and C) of appraisals including the Capability Survey

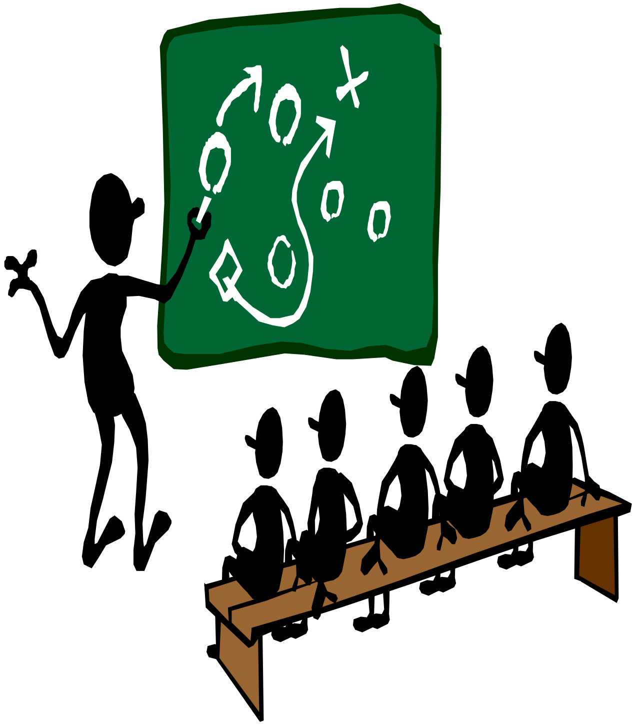
The CERT-RMM Appraiser is responsible to plan and manage the performance of the entire appraisal effort, delegate appraisal tasks to team members, and ensure adherence to CAM appraisal requirements

CERT-RMM Appraisers are sponsored by SEI Partners who are licensed to perform activities on behalf of the SEI



© 2010 Carnegie Mellon University

CERT-RMM Coach



Employees or consultants who are assigned to apply, analyze, champion, manage, contribute, or support CERT-RMM based improvement efforts, appraisal teams, and/or organizational initiatives

Provide a workforce element that will promote a smooth adoption of CERT-RMM concepts to create a sustainable improvement effort

Can deliver CERT-RMM class B or C appraisals and the Capability Survey

© 2010 Carnegie Mellon University

CERT-RMM Navigator

Provide guidance and management of organizations who are applying the CERT-RMM Capability Survey

Coordinator between the organization and the SEI on completion of the Survey and reporting results from the SEI to the organization

Can only deliver the CERT-RMM Capability Survey; no Class appraisals

© 2010 Carnegie Mellon University

CERT-RMM credentialing summary

Role	Authorizations	Path
CERT-RMM Appraiser	--Class A, B, and C --Capability Survey	Reserved for existing CMMI Lead Appraisers only at this time; --Intro to CERT-RMM course --CERT-RMM CAM BootCamp 2011 Program in development for “new” appraisers
CERT-RMM Coach	--Class B and C --Capability Survey	--Intro to CERT-RMM course --CERT-RMM Coach Training
CERT-RMM Navigator	--Capability Survey	--Intro to CERT-RMM course --CERT-RMM Navigator Training
CERT-RMM Appraisal Team Member	Performs as member of appraisal team	--Intro to CERT-RMM course --CERT-RMM Appraisal Team Training

© 2010 Carnegie Mellon University

CERT-RMM and PS-Prep

Comparing and contrasting CERT-RMM in the context of FEMA's PS-Prep program

© 2010 Carnegie Mellon University

What is PS-Prep?

FEMA's Voluntary Private Sector Preparedness Accreditation and Certification Program

Mandated by Title IX of the 9/11 Commission Act of 2007

Participation is completely *voluntary*

DHS approved three standards in June 2010:

- National Fire Protection Association 1600
- British Standard 25999 – Business Continuity Management
- ASIS International SPC.1-2009 – Organizational Resilience: Security Preparedness and Continuity Management System

ANSI-ASQ National Accreditation Board will oversee the certification process

Standards incorporated into and cross-walked in CERT-RMM

© 2010 Carnegie Mellon University

“Prepared” vs. “Capable”

PS-Prep: promote private sector preparedness “including disaster management, emergency management, and business continuity programs.”

CERT-RMM: promote private sector capability—preparedness is a function of:

- Protection strategies (preventative)
- Sustainability strategies (responsive)
- Process institutionalization or “maturity” **to determine the degree to which these strategies will “stick” when the organization is stressed**

Prepared: can you respond?

Capable: can you control your destiny by heading off problems and responding when stressed?

© 2010 Carnegie Mellon University

CERT-RMM vs. ASIS standard -2

A preliminary comparison:

Area of Comparison	CERT-RMM	ASIS SPC.1-2009
Scope	Security, continuity, IT operations; takes management system view but also addresses key operational activities such as vulnerability management, access management, and identity management; also addresses resilience in the development and acquisition phases	Focuses on the organizational resilience management system and key management processes
Process approach	Uses CMMI's process structure; uses "process" as the dimension for measurement of capability; processes are arranged into process areas to allow for scalable and agile adoption	Defines process approach broadly in terms of a "plan-do-check-act model"
Maturity considerations	Uses proven CMMI capability dimension for maturity expression; some process areas express maturity dimensions as well	Includes "maturity" elements, but does not appear to have a maturity representation analogous to CMMI or CERT-RMM
Appraisal	Appraisal against the model uses proven SCAMPI method for CMMI; significant installed base of qualified and experienced appraisers; official "capability level"	Includes an assessment process specific to determining compliance with the standards; no maturity rating

© 2010 Carnegie Mellon University

CERT-RMM scorecard

Advantages:

- **One model** with significant coverage of standards
- Ability to **incorporate any useful standard/practice**
- Capability dimension provides
  - proven **maturity path**
  - ability to determine degree to which practices are retained under stress
- Focuses on **process improvement** not just certification; has a built-in path to improvement
- Allows for **process-based metrics and measurement**

Advantages:

- Creates **internal process improvement experts** to sustain competency
- Appraisal and certification model established and proven; **issued ratings "sanctioned" by the SEI/CERT**

Disadvantage:

- Limited coverage of emergency/crisis management *(for now)*

© 2010 Carnegie Mellon University

CERT-RMM Product Suite

Model artifacts available to begin an adoption process

© 2010 Carnegie Mellon University

CERT-RMM product suite

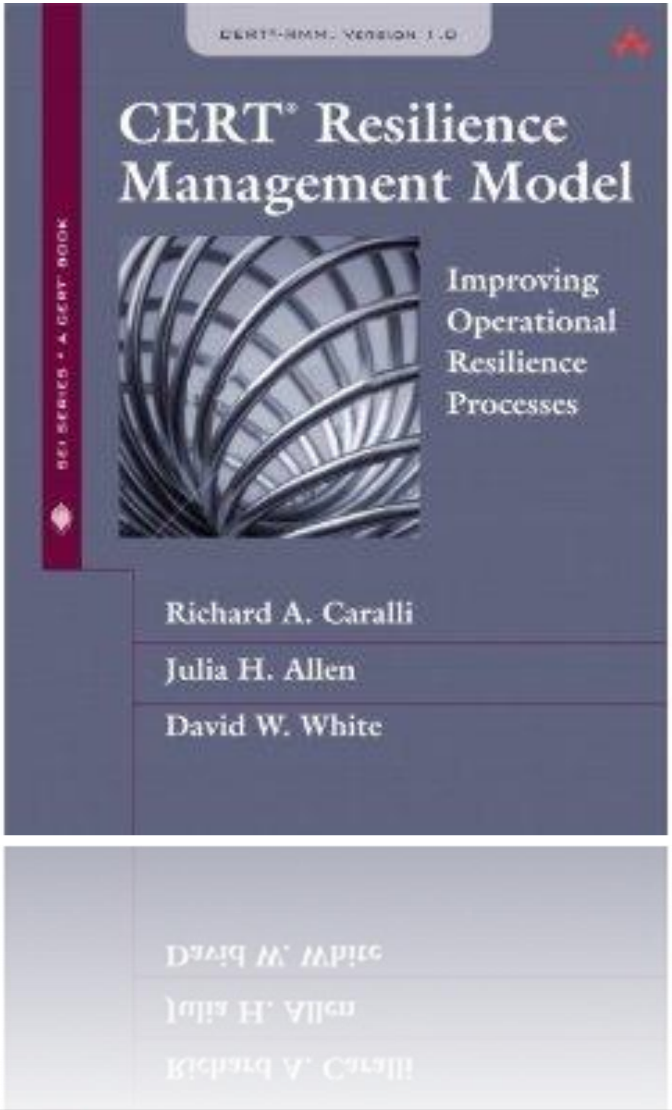
Product	Status
CERT-RMM Model	Version 1.0 released; Technical Report released; individual process areas released @ www.cert.org/resilience
CERT-RMM Capability Appraisal Methodology	Version 1.0 to be released in method description document, August 2010
CERT-RMM Crosswalk	Version 0.95 published; Version 1.0 (expanded) to be published late Summer
Introductory courses	Introduction to CERT-RMM (4 days; offered 4 times/year in Pittsburgh and DC) Executive workshops and tutorials available on demand
Advanced courses	CERT-RMM Intermediate Course (in development for 2011) CERT-RMM CAM BootCamp (pilot scheduled for November 2010) CERT-RMM Role training (Coach, Navigator) CERT-RMM instructor training

© 2010 Carnegie Mellon University

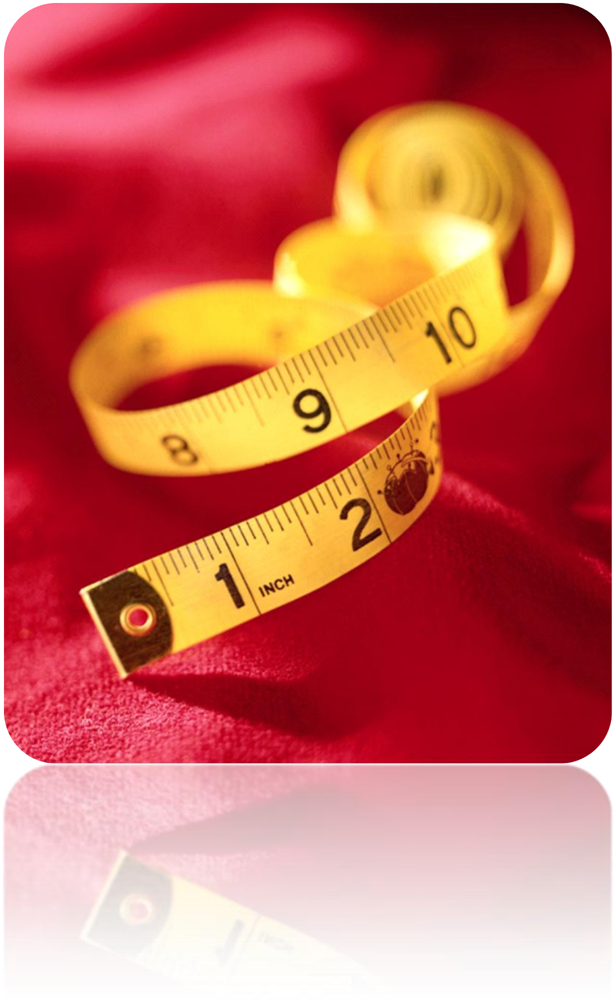
CERT-RMM book publication

Scheduled for publication in November 2010 by Addison-Wesley

Includes full model (v1.0) plus adoption guidance and perspectives of real-world use of the model



Resilience measurement & analysis



Area of research growing out of CERT-RMM development

Focuses on the development of adequate measures to determine transformation of operational resilience management system

Focuses on performance measurement—how well are we doing?

Includes both qualitative and quantitative measurements

Measurement users group (RMM MUG) forming—Fall 2010 opportunity to join a measurement cohort and share

© 2010 Carnegie Mellon University

Questions?

© 2010 Carnegie Mellon University

CERT-RMM contacts

Rich Caralli
RMM Architect and Lead Developer
rcaralli@cert.org

Lisa Young
RMM Appraisal Lead & Developer
lry@cert.org

Richard Lynch
Public Relations — All Media Inquiries
public-relations@sei.cmu.edu

Joe McLeod
For info on working with us
jmcleod@sei.cmu.edu

David White
RMM Transition Lead & Developer
dwhite@cert.org

Julia Allen
RMM Developer/Measurement Team Lead
jha@sei.cmu.edu

SEI Customer Relations
customer-relations@sei.cmu.edu
412-268-5800

© 2010 Carnegie Mellon University

NO WARRANTY

THIS MATERIAL OF CARNEGIE MELLON UNIVERSITY AND ITS SOFTWARE ENGINEERING INSTITUTE IS FURNISHED ON AN “AS-IS" BASIS. CARNEGIE MELLON UNIVERSITY MAKES NO WARRANTIES OF ANY KIND, EITHER EXPRESSED OR IMPLIED, AS TO ANY MATTER INCLUDING, BUT NOT LIMITED TO, WARRANTY OF FITNESS FOR PURPOSE OR MERCHANTABILITY, EXCLUSIVITY, OR RESULTS OBTAINED FROM USE OF THE MATERIAL. CARNEGIE MELLON UNIVERSITY DOES NOT MAKE ANY WARRANTY OF ANY KIND WITH RESPECT TO FREEDOM FROM PATENT, TRADEMARK, OR COPYRIGHT INFRINGEMENT.

Use of any trademarks in this presentation is not intended in any way to infringe on the rights of the trademark holder.

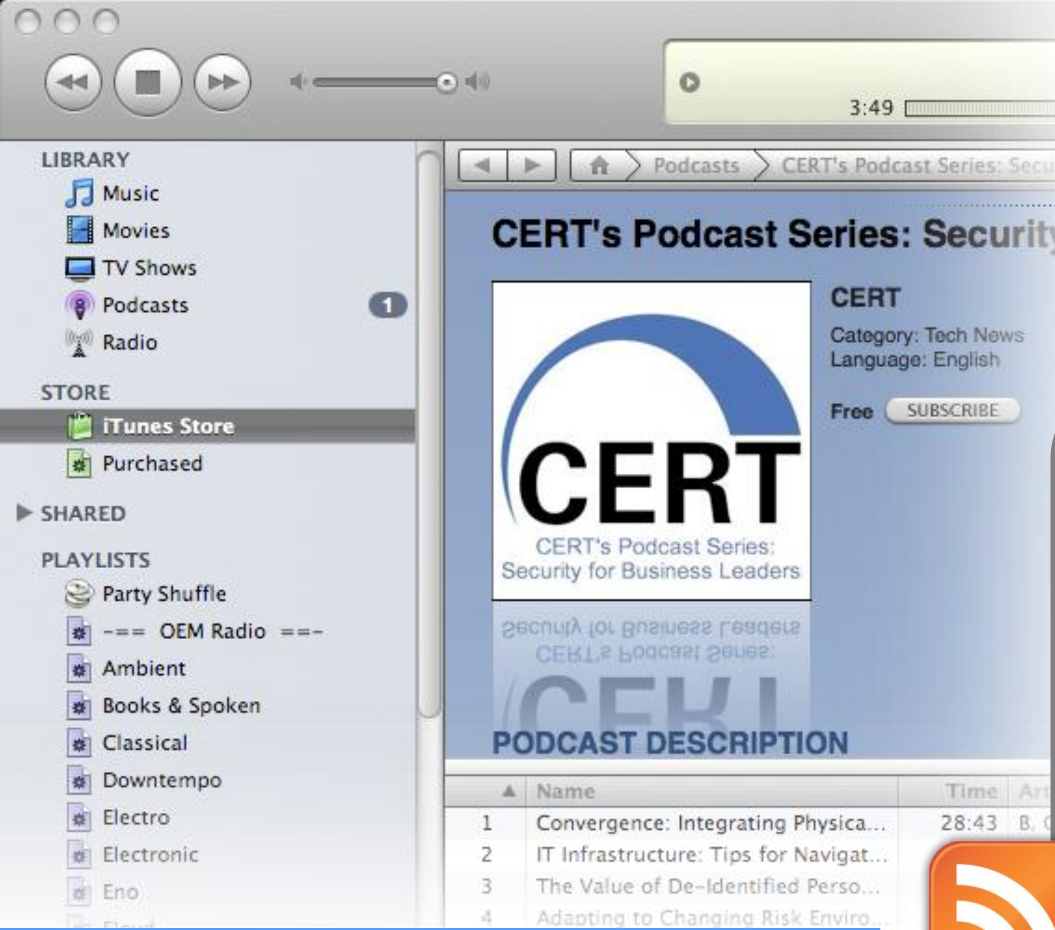
This Presentation may be reproduced in its entirety, without modification, and freely distributed in written or electronic form without requesting formal permission. Permission is required for any other use. Requests for permission should be directed to the Software Engineering Institute at permission@sei.cmu.edu.

This work was created in the performance of Federal Government Contract Number FA8721-05-C-0003 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center. The Government of the United States has a royalty-free government-purpose license to use, duplicate, or disclose the work, in whole or in part and in any manner, and to have or permit others to do so, for government purposes pursuant to the copyright license under the clause at 252.227-7013.

Want a Closer Connection to the SEI?

Become an SEI Member!

▶ www.sei.cmu.edu/membership



CERT's Podcast Series: Security for B

CERT

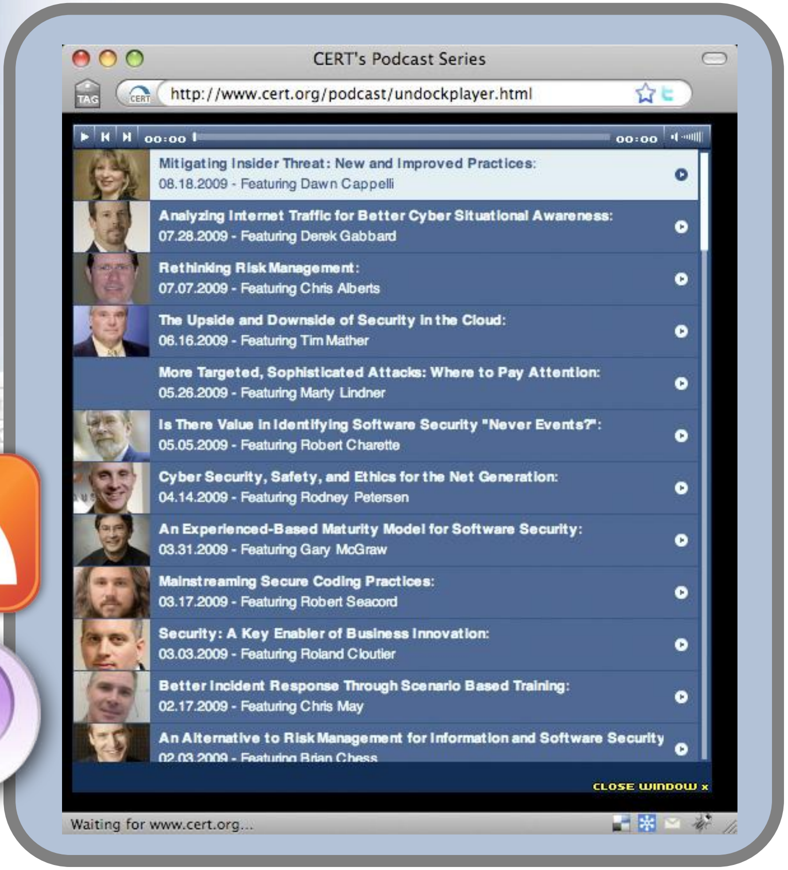
Category: Tech News
Language: English

Free

CERT's Podcast Series: Security for Business Leaders

PODCAST DESCRIPTION

	Name	Time	Art
1	Convergence: Integrating Physica...	28:43	B. C
2	IT Infrastructure: Tips for Navigat...		
3	The Value of De-Identified Perso...		
4	Adapting to Changing Risk Enviro...		

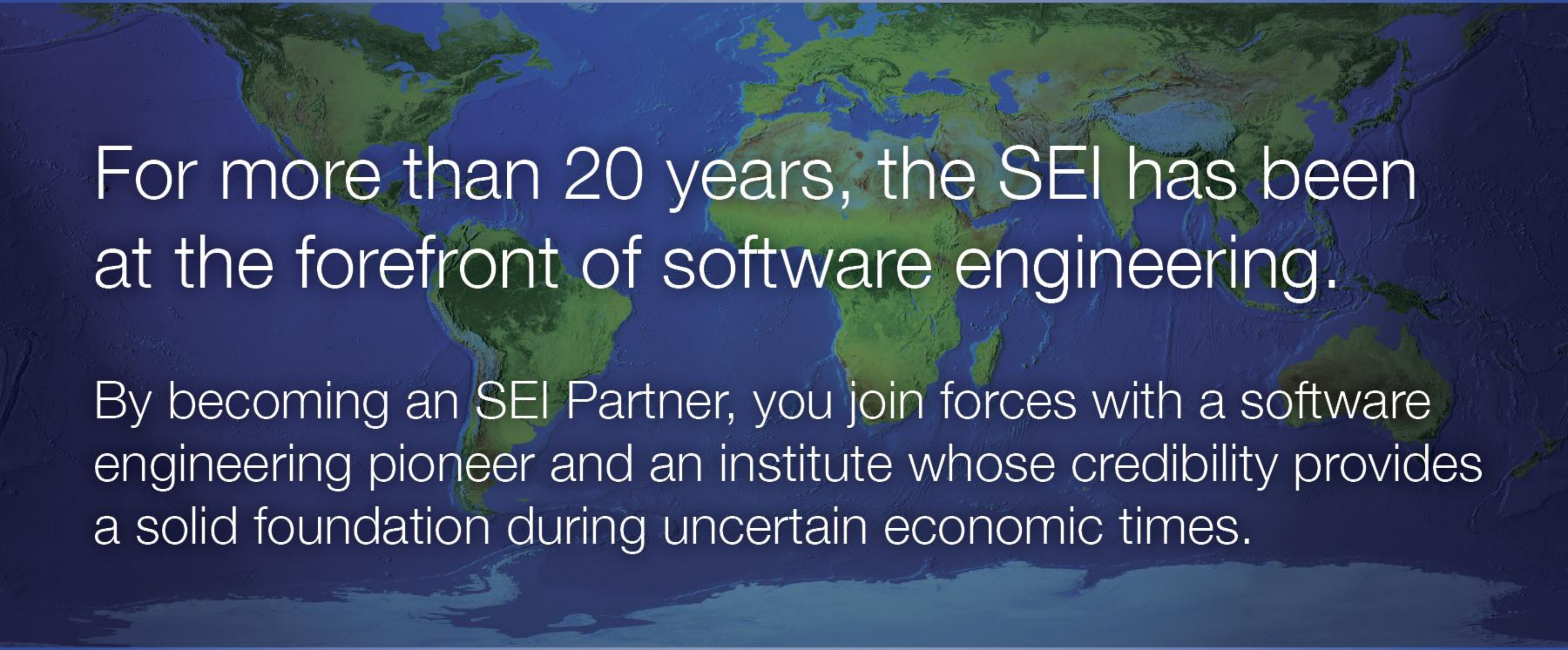

CERT's Podcast Series
http://www.cert.org/podcast/undockplayer.html
00:00
00:00
CLOSE WINDOW x
Waiting for www.cert.org...

- Mitigating Insider Threat: New and Improved Practices: 08.18.2009 - Featuring Dawn Cappelli
- Analyzing Internet Traffic for Better Cyber Situational Awareness: 07.28.2009 - Featuring Derek Gabbard
- Rethinking Risk Management: 07.07.2009 - Featuring Chris Alberts
- The Upside and Downside of Security in the Cloud: 06.16.2009 - Featuring Tim Mather
- More Targeted, Sophisticated Attacks: Where to Pay Attention: 05.26.2009 - Featuring Marty Lindner
- Is There Value in Identifying Software Security "Never Events?": 05.05.2009 - Featuring Robert Charette
- Cyber Security, Safety, and Ethics for the Net Generation: 04.14.2009 - Featuring Rodney Petersen
- An Experienced-Based Maturity Model for Software Security: 03.31.2009 - Featuring Gary McGraw
- Mainstreaming Secure Coding Practices: 03.17.2009 - Featuring Robert Seacord
- Security: A Key Enabler of Business Innovation: 03.03.2009 - Featuring Roland Cloutier
- Better Incident Response Through Scenario Based Training: 02.17.2009 - Featuring Chris May
- An Alternative to Risk Management for Information and Software Security 02.03.2009 - Featuring Brian Chess

CERT's Podcast Series: Security for Business Leaders

www.cert.org/podcast/

© 2010 Carnegie Mellon University



For more than 20 years, the SEI has been at the forefront of software engineering.

By becoming an SEI Partner, you join forces with a software engineering pioneer and an institute whose credibility provides a solid foundation during uncertain economic times.

SEI Partner Network

▶ www.sei.cmu.edu/partners

SEI Training

▶ www.sei.cmu.edu/training